REMEDIACIÓN DE LAS VULNERABILIDADES CRÍTICAS IDENTIFICADAS A PARTIR DE UNA PRUEBA DE INTRUSIÓN A LA INFRAESTRUCTURA TECNOLÓGICA DE UNA ENTIDAD BANCARIA COLOMBIANA

ANA MARÍA SOSSA LÓPEZ
HARVEY ENRIQUE MELO LEÓN

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

REMEDIACIÓN DE LAS VULNERABILIDADES CRÍTICAS IDENTIFICADAS A PARTIR DE UNA PRUEBA DE INTRUSIÓN A LA INFRAESTRUCTURA TECNOLÓGICA DE UNA ENTIDAD BANCARIA COLOMBIANA

ANA MARÍA SOSSA LÓPEZ
HARVEY ENRIQUE MELO LEÓN

Proyecto para optar el título de Especialista en Seguridad Informática

Ing. Álvaro Escobar Escobar
Tutor Temático del Proyecto
Director Especialización en Seguridad Informática
Director Especialización en Telecomunicaciones

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2017

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá D. C. Marzo de 2017.

CONTENIDO

pág.

LISTA DE ANEXOS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE CUADROS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ECUACIONES

Pág.

GLOSARIO

AMENAZA[1]: probabilidad o frecuencia de la ocurrencia de un evento nocivo.

CERT/CC - COORDINATION CENTER OF THE COMPUTER EMERGENCY RESPONSE TEAM: organización dedicada a investigar los errores de software que afectan la seguridad de Internet, publican investigaciones e información de hallazgos y trabaja en conjunto con empresas y gobierno para mejorar la seguridad del software y de internet en general.[2]

FILTRO DE CONTENIDO DE NAVEGACIÓN WEB [3] : software que provee seguridad y productividad respecto a la navegación en internet a través de la restricción de conexiones hacia páginas web no permitidas o permitidas por la organización.

PUBLIC KEY INFRASTRUCTURE (PKI) [4] : tecnología que provee servicios criptográficos a través del uso de algoritmos de cifrado y administración de llaves criptográficas.

RIESGO[5]: impacto relacionado que al explotar una vulnerabilidad podría tener el entorno de un usuario.

SANS: organización líder en formación de seguridad Informática, conocida por proporcionar entrenamiento intensivo diseñado para profesionales y empresas que requieran dominar los pasos prácticos para defender sistemas y redes.[6]

---

[1] MELL, Peter; SCARFONE, Karen, National Institute of Standards and Technology y ROMANOSKY, Sasha. Carnegie Mellon University A Complete Guide to the Common Vulnerability Scoring System Version 2.0. [en línea]. CVSS, June 2007. Disponible en internet: URL< https://www.first.org/cvss/cvss-v2-guide.pdf>

[2] CERT, Software Engineering Institute Carnegie Mellon University. Vulnerability Notes Database Field Description. [en línea]. Cert. Disponible en Internet: URL <http://www.kb.cert.org/vuls/html/fieldhelp>

[3] ALVEY, Robert. The Art of Web Filtering [en línea]. GSEC Practical v1.4b. SANS Institute InfoSec Reading Room, February 9, 2004. Disponible en Internet: URL <https://www.sans.org/reading-room/whitepapers/bestprac/art-web-filtering-1375>

[4] SANS Institute InfoSec Reading Room, PKI, The What, The Why, and The How. [en línea]. SANS. Disponible en Internet: URL<https://www.sans.org/reading-room/whitepapers/vpns/pki-what-why-764>.

[5] MELL, Peter; SCARFONE, Karen, National Institute of Standards and Technology y ROMANOSKY, Sasha. Carnegie Mellon University A Complete Guide to the Common Vulnerability Scoring System Version 2.0. [en línea]. CVSS, June 2007. Disponible en internet: URL< https://www.first.org/cvss/cvss-v2-guide.pdf>

[6] https://www.sans.org/about/why-sans/

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)[7]: es un sistema hibrido que combina dos productos de seguridad: el Security Información Management (SIM) que se encarga de políticas y cumplimiento de estándares a través de la consolidación de Logs y el Security Event Management (SEM) el cual provee soporte técnico para la administración de amenazas, eventos e incidentes de seguridad en tiempo real.

SISTEMA DE ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES[8]: Mobile Device Management (MDM por sus siglas en inglés), es un mecanismo por el cual las corporaciones pueden mantener control sobre los datos corporativos en los dispositivos móviles, así como proveer acceso seguro a los recursos de cómputo empresariales.

SISTEMA DE DETECCIÓN DE INTRUSOS[9]: Intrusión Prevention System (IPS por sus siglas en inglés) es un sistema usado para descartar o dropear activamente paquetes de datos, desconectar conexiones de red que contienen datos no autorizados o paquetes maliciosos.

VULNERABILIDAD [10] : error, falla, debilidad, o exposición de una aplicación, sistema, dispositivo o servicio que podría llevar a un fallo en la confidencialidad, integridad, o disponibilidad.

[7] KIBIRKSTIS, Algis. What is The Role of a SIEM in Detecting Events of Interest. [en línea]. SANS IDFAQ, November 2009. Disponible en internet: URL<https://www.sans.org/security-resources/idfaq/what-is-the-role-of-a-siem-in-detecting-events-of-interest/5/10>.

[8] COLLYER, Tim. Airwatch MDM and Android: a policy and technical review. [en línea]. GSEC. SANS Institute InfoSec Reading Room July 11. 2014. Disponible en Internet: URL <https://www.sans.org/reading-room/whitepapers/pda/airwatch-mdm-android-policy-technical-review-35372>.

[9] HOLLAND, Ted. Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth [en línea]. GSEC Practical v1.4b, Option 1, SANS Institute InfoSec Reading Room, February 23, 2004. Disponible en Internet: URL <https://www.sans.org/reading-room/whitepapers/detection/understanding-ips-ids-ips-ids-defense-in-depth-1381>.

[10] MELL, Peter; SCARFONE, Karen, National Institute of Standards and Technology y ROMANOSKY, Sasha. Carnegie Mellon University A Complete Guide to the Common Vulnerability Scoring System Version 2.0. [en línea]. CVSS, June 2007. Disponible en internet: URL< https://www.first.org/cvss/cvss-v2-guide.pdf>

RESUMEN

Este trabajo busca definir un plan de remediación a las vulnerabilidades críticas identificadas en la prueba de intrusión realizada a la infraestructura tecnológica de una entidad bancaria colombiana en octubre del año 2016. Para la elaboración del plan de remediación se desarrolló una metodología que permite identificar el riesgo asociado a cada vulnerabilidad reportada, permitiendo priorizar la remediación de las vulnerabilidades que representan un alto riesgo para el Banco, así como definir los controles que deben ser implementados para mitigar los riesgos garantizando que el riesgo residual cumple con los niveles aceptables de riesgo de la entidad.

Nota: Se realiza cambio en el nombre de la entidad bancaria y la información como direcciones ip, nombre de servidores, usuarios y dominios; ya que esta información es información confidencial de Banco.

INTRODUCCIÓN

Las entidades prestadoras de bienes y servicios financieros en busca de brindar un mejor servicio a los consumidores y con miras a incrementar su participación en el mercado, constantemente acondicionan sus procesos, servicios, canales electrónicos e infraestructura tecnológica, con el fin de apoyar las necesidades del negocio.

Desde lo propio de la Infraestructura de TI, las entidades constantemente acondicionan su infraestructura tecnológica de tal forma que sea posible apoyar las iniciativas estratégicas de la entidad, esto conlleva a cambios en el estado de seguridad de los componentes de TI, así como deterioro en los controles de seguridad implementados, por lo cual y en cumplimiento de la legislación Colombiana (Circular 042 Superintendencia Financiera de Colombia) [11] las entidades anualmente realizan como mínimo una prueba de intrusión a los componentes de infraestructura tecnológica con el fin de identificar los nuevos riesgos de Seguridad de la Información que puedan ser materializados.

A diferencia de un análisis de vulnerabilidades, una prueba de Intrusión tiene como objetivo comprobar la materialización del riesgo por medio de la explotación de las vulnerabilidades y/o debilidades identificadas por una entidad externa experta en seguridad, sobre los componentes de infraestructura tecnológica; esto permite conocer el estado y efectividad real de los controles de seguridad existentes, así como identificar las oportunidades de mejora que deben ser implementadas en los controles de seguridad establecidos, con el fin de evitar que la infraestructura tecnológica sea comprometida por un atacante mal intencionado afectando la confidencialidad, integridad y disponibilidad de la información.

[11] SUPERINTENDENCIA Financiera de Colombia. Requerimientos mínimos de seguridad y calidad para la realización de operaciones. Circular Externa 042 de 2012 [en línea]. Superintendencia Financiera de Colombia. Octubre, 2012. Disponible en Internet: URL< http://www.certicamara.com/download/correspondencia/20121005_Anexos_12_circular_042_de_2012.pdf>

1. TÍTULO

La mitigación de los riesgos de seguridad de la información identificados en la prueba de intrusión realizada en octubre del 2016 en una entidad bancaria colombiana, amerita el estudio de los controles a implementar para las vulnerabilidades críticas, así como el diseño de una metodología para la gestión del proceso de Gestión de Vulnerabilidades de Pruebas de Intrusión. Por lo anterior el trabajo se ha titulado: “Remediación de las vulnerabilidades críticas identificadas a partir de una prueba de intrusión a la infraestructura tecnológica de una entidad bancaria colombiana”

2. JUSTIFICACIÓN

El fundamento de esta investigación nace de la necesidad de solucionar de manera eficiente las debilidades y vulnerabilidades presentes en la infraestructura tecnológica de una entidad bancaria.

De acuerdo con una revisión realizada por Asobancaria respecto a los niveles de fraude reportados anualmente por las diferentes instituciones que brindan servicios financieros, se puede observar que el fraude electrónico se encuentra creciendo exponencialmente desde el año 2010 llegando a registrar pérdidas hasta de USD 50 Millones para el año 2015 en Colombia; existe registro de algunos fraudes electrónicos realizados a nivel mundial en los cuales se pudo comprobar que el robo fue realizado a través del compromiso (Hackeo) de componentes de infraestructura tecnológica mediante la explotación de vulnerabilidades y la utilización malware avanzado como fue el caso del Robo de 73 Millones de dólares al Banco de Bangladesh[12][13], y el robo de 12 millones de dólares del Banco del Austro en ecuador en el año 2016 por medio de la plataforma Swift[14].

En la actualidad existe una gran motivación por parte de los ciberdelincuentes para atacar la infraestructura tecnológica de las entidades financieras ya que es posible realizar fraude electrónico desde múltiples procesos de negocio ejecutados en el BackOffice a través de plataformas tecnológicas como Swift, ACH, PSE, entre otros; esto es atractivo para los ciberdelincuentes ya que representa una fuente potencial de ingresos, mucho más rentable y menos riesgosa que otras actividades delictivas como el tráfico de estupefacientes, o el tráfico de armas.

[12] CROMO. Así fracasó el robo informático al Banco de Bangladesh. [en línea]. Cromo. Abril 27, 2016. Disponible en Internet: URL<http://www.cromo.com.uy/asi-fracaso-el-robo-informatico-al-banco-bangladesh-n902149>

[13] EL PAIS, Los piratas que robaron 73 millones al banco central de Bangladesh 'hackearon' una impresora clave. [en línea]. El País. Marzo 17, 2016. Disponible en Internet: URL<http://economia.elpais.com/economia/2016/03/17/actualidad/1458200294_374693.html>

[14] MUY SEGURIDAD.NET. Roban 12 millones de dólares tras hackear un banco de Ecuador. [en línea]. Muy Seguridad.net. Mayo 24, 2016 Disponible en Internet: URL <http://muyseguridad.net/2016/05/24/roban-12-millones-dolares-hackear-banco-ecuador/>

3. PLANTEAMIENTO DEL PROBLEMA

El sector financiero constantemente está generando nuevos productos y servicios financieros que requieren modificación de los controles de seguridad interna y perimetrales implementados, así como cambios en la infraestructura tecnológica que soporta los canales de prestación de servicios como el canal de internet, los ATM, Oficinas, Swift, Corresponsales Bancarios, Convenios (Clientes Empresariales) y proveedores entre otros; estos cambios modifican el estado natural (Estado inicial) de la seguridad de los componentes de infraestructura tecnológica generando nuevos vectores de ataque que pueden ser utilizados por los ciberdelincuentes para diversos fines como generar indisponibilidad de las plataformas tecnológicas, obtener información sensible de la organización y/o de los clientes y realizar fraudes electrónicos entre otros.

A pesar de las grandes inversiones en infraestructura de seguridad realizadas por las entidades financieras para evitar ser víctimas de intrusiones y/o accesos no autorizados, los Ciberdelincuentes constantemente investigan y desarrollan nuevas formas de evadir los controles de seguridad para comprometer los componentes de infraestructura tecnológica.

Para la entidad financiera en la cual se desarrolla esta investigación, el área de Seguridad Informática administra algunos componentes de infraestructura tecnológica de seguridad como IPS, MDM, WebFiltering, PKI, SIEM, entre otros, esto permite ejecutar las acciones o controles que correspondan de manera autónoma sobre estos componentes, sin embargo existen algunos controles que se deben implementar en diferentes capas de TI como los sistemas operativos, Bases de datos, contenedores de aplicación, aplicaciones in house, Firewall, Switches, etc. Así mismo existen controles que no pueden ser ejecutados en el corto plazo puesto que se requiere realizar un proyecto, pruebas de concepto, etc. Por estas razones el alcance de esta investigación es la aprobación por parte de la entidad financiera de las medidas y/o controles a implementar para remediar las vulnerabilidades críticas identificadas en la prueba de intrusión, con el fin de evitar ataques futuros que comprometan la confidencialidad, integridad y disponibilidad de la información.

A continuación se presenta la pregunta problema:

¿Qué controles y/o Configuraciones de los componentes de Infraestructura tecnológica deben ser implementados en esta entidad financiera para reducir a

niveles aceptables los riesgos de seguridad de la información conforme a las directrices establecidas en la norma ISO27005?

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar un plan de remediación para las vulnerabilidades críticas identificadas y reportadas en octubre de 2016 en una prueba de intrusión a la infraestructura tecnológica de una entidad bancaria colombiana.

4.2 OBJETIVOS ESPECÍFICOS

- Definir una metodología especifica que permita llevar a cabo el tratamiento y remediación de las vulnerabilidades críticas detectadas y/o explotadas en la prueba de intrusión realizada en octubre del 2016.

- Realizar una clasificación de las vulnerabilidades detectadas y reportadas de acuerdo a su criticidad e impacto.

- Definir el control técnico a implementar que remedia o mitiga los riesgos asociados a las vulnerabilidades críticas.

- Diseñar el plan de remediación para cada vulnerabilidad critica reportada en la prueba de intrusión.

5. MARCO TEÓRICO

5.1 METODOLOGÍA DE PRUEBAS DE INTRUSIÓN

Las pruebas de intrusión se realizan con el objetivo de medir el nivel de seguridad y madurez de los controles implementados en una organización a fin de evitar accesos no autorizados a los sistemas operativos, aplicaciones o bases de datos y a su información confidencial. Las pruebas de intrusión tienen la capacidad de simular el alcance que puede llegar a tener un potencial atacante de forma remota o local sobre la infraestructura de una entidad, el cual busca explotar de forma activa las vulnerabilidades de seguridad de dicha infraestructura

Las pruebas de intrusión se realizan en un ambiente controlado que permita simular un ataque permitiendo conocer el nivel de seguridad de la entidad, así:

- Nivel de Tolerancia: Resistencia de los sistemas a ataques que no afecten su funcionamiento.
- Nivel de Complejidad: Grado de dificultad de los ataques para afectar un sistema.
- Nivel de Detección: Capacidad de la infraestructura de seguridad para detectar los ataques[15].

Los alcances de las pruebas de penetración están dados por el éxito obtenido al evadir los controles de red implementados, escalar privilegios, realizar análisis e identificación de servicios y a su vez identificar las vulnerabilidades asociadas en los sistemas y redes de la infraestructura tecnológica

Para el desarrollo de las pruebas de intrusión en la entidad se siguen las siguientes fases y ciclos los cuales van desde realizar un descubrimiento de la

[15] PROTEKTNET, Pruebas de Penetración. [en línea]. Protektnet. Disponible en Internet: URL<https://protektnet.com/servicios/analisis-de-seguridad/pruebas-de-penetracion/>

infraestructura, conocer sus activos críticos hasta llegar a realizar la explotación de las vulnerabilidades descubiertas[16].

FASE I: Evasión de controles de acceso a la red

Como primera fase se debe conseguir saltar los controles de acceso a la red que se tengan implementados en los equipos de la organización, a continuación en el cuadro 1 se muestran algunas tareas que se pueden aplicar para lograr evadir estos controles[17]:

Cuadro 1. Evasión de controles de acceso a la red

Objetivo	Actividades
Evasión del control de acceso a la red	Inspección de Puertos físicos y en funcionamiento
	Inspección de elementos de software que determinan la salud de un equipo
	Inspección de puertos Ethernet
	Inicio del equipo con otro sistema operativo
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

FASE II: Escalar privilegios de forma remota

Una vez se tenga acceso a un equipo de red de la entidad, se debe garantizar lograr de forma exitosa la autenticación a otras máquinas de la red con usuarios locales y/o de dominio, para lo cual algunas tareas mostradas en el cuadro 2 son usadas para obtener el passwords de los usuarios.

Cuadro 2. Escalar privilegios de forma remota

Objetivo	Actividades
Escalar	Credenciales cacheadas localmente

[16]Informe de pruebas de intrusión Memorando Interno de la entidad 0302-MEM-00102-15-121[Confidencial]
[17] ARKIN, Ofir. Evasión de controles de NAC Network Access Control. [en línea]. Insightix. 2006-2007 Disponible en Internet: URL<https://www.blackhat.com/presentations/bh-dc-07/Arkin/Presentation/bh-dc-07-Arkin-ppt-up.pdf>

privilegios de forma remota	Cracking de hashes obtenidos
	Log's de servicios, aplicaciones y sistema operativo
	Volcado de memoria
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

FASE III: Descubrimiento de activos y servicios

Luego de obtener las credenciales de autenticación que permiten acceder a otros equipos de la red se puede realizar un descubrimiento de los segmentos de red con los que se tiene conectividad, información que permite indagar los puertos abiertos e inferir los servicios activos, en el cuadro 3 se presentan algunas de las actividades con las que se puede realizar el descubrimiento de activos y servicios:

Cuadro 3. Inspección externa de dispositivos y sistemas

Objetivo	Actividades
Inspección externa de dispositivos y sistemas	Análisis de cada puerto abierto con el servicio y protocolo correspondiente
	Uso de analizadores de protocolos (NMAP versioning)
	Identificación de servicios de acceso remoto VPN
	Identificación de servicios de capa física, enlace y de red
	Verificación de las aplicaciones de los sistemas y sus versiones
	Localizar e identificar remapeos y re direccionamientos
	Identificación componentes (TCP / UDP)
	Ejecución servicios UDP (over RCP) Aplicaciones
	Identificación de dispositivos, sistemas y plataformas
	Footprinting y Fingerprinting de servicios, servidores y aplicaciones
	Verificación de servicios publicados de manera inconsciente (Shodan, Robtex, Google)
	Búsqueda de errores y configuraciones por defecto
	Mapeo inicial de la red
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

FASE IV Inspección y explotación de vulnerabilidades

Por último con base en la información recolectada en la anterior fase, esta es utilizada para indagar las vulnerabilidades conocidas sobre las versiones de los servicios usados y/o sistemas operativos.

En el cuadro 4 se presentan algunas de las tareas que se utilizan para realizar la inspección y detección de vulnerabilidades.

Cuadro 4. Inspección de vulnerabilidades

Objetivo	Actividades
Inspección de vulnerabilidades	Detección y búsqueda de firma de fallos y vulnerabilidades en sistemas operativos
	Análisis de estado de actualizaciones en sistemas operativos
	Análisis de Servicios críticos en la organización
	Servicios SMTP y acceso a Correo.
	Servicios DNS
	Servidores FTP
	Servidores de base de datos
	Servidores de VPN
	Servidores web
	Servidores de directorio activo
	Servicios de monitorización
	Servicios basados en telefonía IP (VOIP)
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Para realizar la explotación una vez identificada la vulnerabilidad y confirmado que es posible explotarla se siguen las siguientes tareas presentadas en el cuadro 5:

Cuadro 5. Explotación de Vulnerabilidades

Objetivo	Actividades
Explotación de vulnerabilidades	Se realizarán pruebas de ataque con exploits basados en las posibles vulnerabilidades detectadas
	Se realizarán pruebas basadas en ataques de red basadas en IPV4 e IPV6, ataques como: MITM, DHCP spoofing, Hijacking, modificación de paquetes.
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Para el tratamiento de cada una de las vulnerabilidades reportadas a partir de una prueba de intrusión, existen proyectos internacionales dedicados a informar y actualizar los controles que se deben considerar al momento de mitigar o subsanar vulnerabilidades. Los siguientes son algunos proyectos y metodologías:

- OSSTMM Open Source Security Testing Methodology Manual.
- OWASP Open Web Application Security Project.
- ISSAF Information Systems Security Assessment Framework.
- NIST 800-115 Technical Guide to Information Security Testing and Assessment.
- OWISAM Metodología WiFi.

Las siguientes son listas de vulnerabilidades específicas o tipos de vulnerabilidades genéricas que tiene por objeto proporcionar nombres comunes a los problemas conocidos públicamente:

- CVE Common Vulnerabilities and Exposures.
- CWE Common Weakness Enumeration.
- CAPEC Common Attack Pattern Enumeration and Classification son listas de vulnerabilidades específicas.

Para establecer las clasificaciones del impacto, la NVD - Base de Datos Nacional de Vulnerabilidades recomienda tomar como punto de referencia los scores establecidos por la CVSS, los cuales se presentan en la tabla 1:

Tabla 1. Clasificaciones de las vulnerabilidades según el impacto

Etiqueta	Score
Vulnerabilidad critica	9.6 - 10.0
Vulnerabilidad alta	7.0 - 9.5
Vulnerabilidad media	4.0 - 6.9
Vulnerabilidad baja	0.1 - 3.9
Vulnerabilidad información	0.0
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Basados en el Modelo de Madurez de Conciencia de Seguridad de SANS y el Modelo de Madurez de Gobierno de Seguridad en TI se define los siguientes niveles para la medición de resultados obtenidos en la prueba de intrusión[18]:

- Bajo: No existes controles de seguridad.
- Medio-Bajo: Existen controles de seguridad, pero no son formales.
- Medio: Controles de seguridad formales con acciones de mejora.
- Medio-Alto: Implementación de controles de calidad en seguridad.
- Alto: Medición y mejoramiento continuo basado en métricas e indicadores.

5.2 METODOLOGÍA DE GESTIÓN DE RIESGO

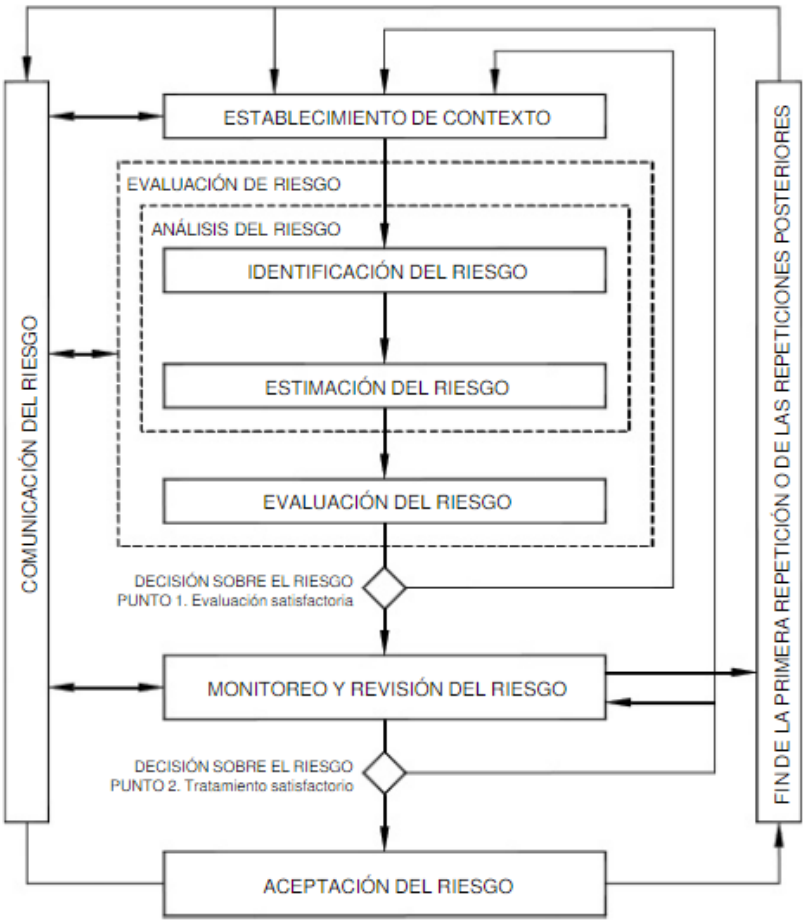
La metodología ISO 27005 establece un proceso iterado de gestión de riesgos de seguridad de la información que contiene las siguientes actividades:

- Establecimiento del contexto.
- Valoración del riesgo.
- Tratamiento del riesgo.
- Aceptación del riesgo.
- Comunicación del riesgo.
- Monitoreo y revisión continuos de los riesgos.

Como se muestra en la figura 1, éste proceso permite realizar múltiples iteraciones para las actividades de valoración y/o tratamiento del Riesgo, lo cual permite tratar los riesgos altos de manera correcta, a continuación se presenta el proceso propuesto en la norma:

[18] SANS, Securing the Human. Defining the Security Awareness Maturity Model. [en línea]. SANS. Mar 8, 2016 Disponible en Internet: URL<https://securingthehuman.sans.org/blog/2016/03/08/defining-the-security-awareness-maturity-model>
http://www.colmich.edu.mx/computo/files/MAAGTIC/risk_it_framework.pdf pag. 42

Figura 1. Proceso de gestión del riesgo en la seguridad de la información



Fuente: Autores ISO 27005, Proceso de gestión del riesgo en la seguridad de la información.

La norma ISO 27005 alinea el proceso de gestión de riesgos de seguridad en el proceso PHVA (Planificar, Hacer, verificar y actuar) del Sistema de Gestión de

seguridad de la información (SGSI por sus siglas en español) -ISO 27001 como se muestra en la tabla 2:

Tabla 2. Alineamiento del SGSI y el proceso de gestión del riesgo en la seguridad de la información

Proceso de SGSI	Proceso de gestión del riesgo en la seguridad de la información
Planificar	Establecer el contexto Valoración del riesgo Planificación del tratamiento del riesgo Aceptación del riesgo
Hacer	Implementación del plan de tratamiento del riesgo
Verificar	Monitoreo y revisión continuos de los riesgos
Actuar	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información
Fuente: Autores ISO 27005. Alineamiento del SGSI y el proceso de Gestión del Riesgo en la Seguridad de la Información.	

5.2.1 Establecimiento del contexto. Esta actividad consiste en definir el alcance y los límites de la gestión de riesgos de Seguridad de la Información, basándose en los objetivos, procesos y funciones de negocio, así como la estructura de la organización, requisitos legales, normativos y políticas de la organización.

Para establecer el contexto es esencial determinar el propósito de la gestión del riesgo, este propósito podría ser:

- Dar soporte a un SGSI.
- Conformidad legal y evidencias de la debida diligencia;
- Preparación de un plan para la continuidad del negocio;
- Preparación de un plan de respuesta a incidentes;
- Descripción de los requisitos de seguridad de la información para un producto, un servicio o un mecanismo.

La norma recomienda desarrollar el contexto a partir de los siguientes enfoques:

- Evaluación de riesgos. Desarrollar criterios de evaluación de riesgo teniendo en cuenta el valor estratégico del proceso de información del negocio, criticidad de los activos de información involucrados, requisitos legales, consecuencias en el buen nombre, confidencialidad, integridad y disponibilidad para las operaciones del negocio, entre otros.
- Criterios de Impacto. Desarrollar criterios de impacto a través de la clasificación de activos de información impactados, perdida del negocio y del valor financiero, daños en la reputación e incumplimiento de requisitos legales.
- Criterios de Aceptación de Riesgos. Desarrollar criterios de aceptación del riesgo teniendo en cuenta los requerimientos legales, relación entre el beneficio y el riesgo, umbrales con meta de nivel deseable, requisitos para el tratamiento adicional en el futuro.

Algunos ejemplos de contexto puede ser una aplicación del negocio, infraestructura tecnológica, un proceso de negocio, etc.

5.2.2 Valoración del riesgo en la seguridad de la información. Esta actividad requiere que se haya definido el contexto claramente, los riesgos se deben identificar y describir cuantitativamente o cualitativamente y priorizar frente a los criterios de evaluación del riesgo.

La valoración del riesgo consta de tres actividades:

5.2.3 Análisis de riesgo. Esta subactividad se divide en las siguientes 2 actividades:

- Identificación del riesgo. Busca determinar que podría suceder que cause perdida potencial, como dónde y por qué podría ocurrir la perdida, para esto se deben realizar las siguientes actividades:

  - Identificación de activos. Identificar los propietarios de los activos de información y adjudicar la responsabilidad.
  - Identificación de amenazas. Múltiples fuentes como el propietario del activo de información, incidentes de seguridad consultoría, entre otros.
  - Identificación de los controles existentes. Revisión de los documentos que contengan información sobre los controles, verificación con los responsables de

Seguridad de la información de la entidad, revisión de las auditorías internas, entre otros.

- Identificación de vulnerabilidades. Identificar las vulnerabilidades que pueden ser explotadas por las amenazas en los activos de información.
- Identificación de las consecuencias. Identificar las consecuencias que pueden traer las pérdidas de confidencialidad, integridad y disponibilidad de la información de los activos de información.

- Estimación del riesgo: Puede ser cuantitativa o cualitativa o una combinación de ambas.

  Estimación Cualitativa: Se utiliza una escala de atributos calificativos para describir la magnitud de las consecuencias potenciales, por ejemplo Bajo, alta, media, etc.

  Estimación Cuantitativa: Se utiliza una escala de valores numéricos para calificar la magnitud de las consecuencias potenciales.

- Evaluación de consecuencias. puede estimarse con respecto al valor de reemplazo del activo y/o las consecuencias para el negocio por la pérdida o compromiso del activo.
- Evaluación de la probabilidad de incidentes. Considera la frecuencia con la que ocurren las amenazas y la facilidad con las que las vulnerabilidades pueden ser explotadas teniendo en cuenta las fuentes de amenazas accidentales, fuentes de amenazas deliberadas, vulnerabilidades y controles existentes.
- Nivel de estimación de riesgo. Asigna valores a la probabilidad y las consecuencias de un riesgo.

5.2.4 Evaluación del riesgo. Esta actividad se divide en 2 sub actividades:

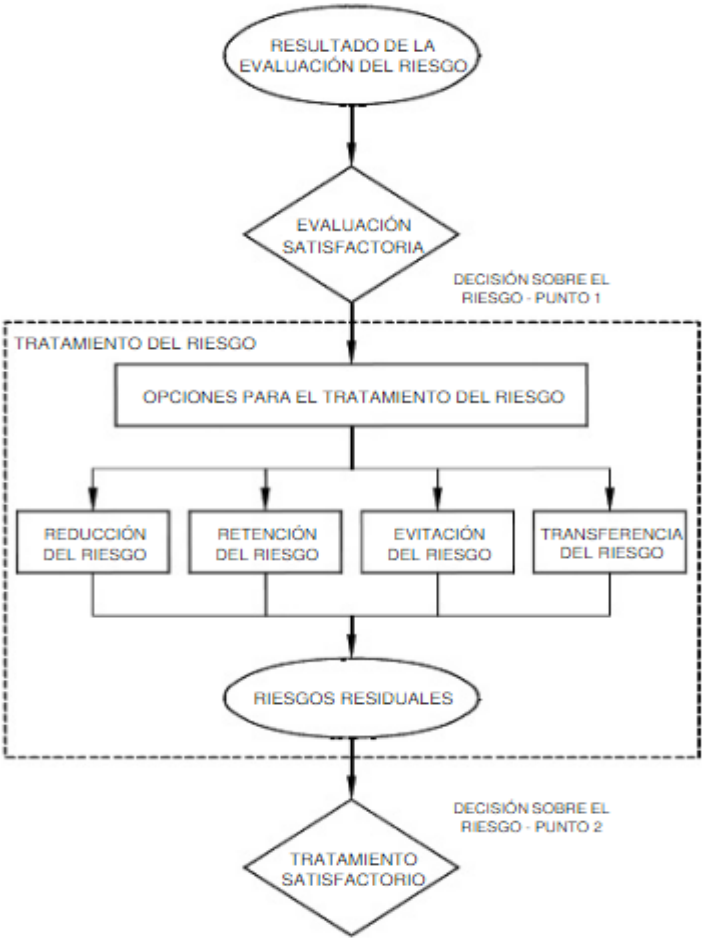
- Propiedades de la seguridad de la información. si un criterio no es importante para la organización (por ejemplo la pérdida de confidencialidad), entonces todos los riesgos que tienen impacto sobre este criterio pueden no ser importantes.

- La importancia de los procesos del negocio o de la actividad sustentada por un activo. si se determina que el proceso tiene importancia baja, los riesgos asociados con él deberían tener una consideración más baja que los riesgos que tienen impacto en procesos o actividades más importantes.

5.2.5 Tratamiento del riesgo en la seguridad de la información. Esta actividad consiste en seleccionar los controles para reducir, retener, evitar o transferir los riesgos, así como definir un plan para el tratamiento de riesgo.

En la Figura 2 se presenta en resumen de la actividad de tratamiento de riesgo:

Figura 2. Actividad para el tratamiento del riesgo



Fuente: Autores ISO 27005, Actividad para el tratamiento del riesgo.

Las opciones para el tratamiento del riesgo se deben ser seleccionadas con base en la evaluación del riesgo, el costo esperado para implementar estas opciones y los beneficios esperados como resultado de tales opciones, las cuatro formas de tratar el riesgo no necesariamente funcionan de manera independiente, un riesgo pude ser tratado de múltiples formas de manera simultánea.

- Reducción del Riesgo. Para reducir el riesgo se deben seleccionar controles que disminuyan el riesgo residual a un nivel aceptable por la organización, se debe considerar varias restricciones como las siguientes al momento de seleccionar los controles:

  - Restricciones de tiempo, restricciones financieras, restricciones técnicas, restricciones operativas, restricciones culturales, restricciones éticas, percepciones ambientales, restricciones legales, facilidad de utilización, restricciones personales, restricciones para la integración de controles nuevos y existentes.

- Retención del Riesgo. El nivel de riesgo satisface los criterios para su aceptación, por lo cual no es necesario implementar controles adicionales.
- Evitación del Riesgo. Cuando los riesgos se consideran muy altos, o si los costos para implementar otros controles exceden los beneficios se puede tomar la decisión para evitar por completo el riesgo.
- Transferencia del Riesgo. La transferencia del riesgo consiste en compartir algunos riesgos con partes externas, usualmente mediante un seguro que dará soporte a las consecuencias o mediante la subcontratación de un asociado cuya función será monitorear los sistemas de información y tomar las acciones que corresponda para detener un ataque que produzca un novel definido de daño.

5.2.6 Aceptación del riesgo en la seguridad de la información. Esta actividad comprende la toma de decisión de aceptar los riesgos y las responsabilidades de la decisión, los directivos de la entidad deben revisar y aprobar los planes propuestos para el tratamiento del riesgo y los riesgos residuales resultantes.

5.2.7 Comunicación de los riesgos para la seguridad de la información. Esta actividad trata acerca de informar, intercambiar y compartir con todas las partes involucradas los riesgos de la organización.

Los objetivos principales de la comunicación del riesgo son:

- Brindar seguridad del resultado de la gestión del riesgo de la organización;
- Recolectar información sobre el riesgo;
- Compartir los resultados de la evaluación del riesgo y presentar el plan para el tratamiento del riesgo;
- Evitar o reducir tanto la ocurrencia como la consecuencia de las brechas en la seguridad de la información debidas a la falta de comprensión mutua entre quienes toman las decisiones y las partes involucradas;
- Brindar soporte para la toma de decisiones;
- Obtener conocimientos nuevos sobre la seguridad de la información.

5.2.8 Monitoreo y revisión del riesgo en la seguridad de la información. Esta actividad hace referencia a como los riesgos y sus factores (el valor de los activos, los impactos, las amenazas, las vulnerabilidades, la probabilidad de ocurrencia) se deben monitorear y revisar con el fin de identificar todo cambio en el contexto de la organización en una etapa temprana.

5.2.9 Monitoreo y revisión de los factores de riesgo. Debido a que los riesgos no son estáticos, es necesario el monitoreo constante para detectar estos cambios, las entidades deben garantizar el monitoreo continuo de los siguientes aspectos:

- Modificaciones necesarias de los valores de los activos.
- Amenazas nuevas que podrían estar activas tanto fuera como dentro de la organización y que no se han evaluado.
- Probabilidad de que las vulnerabilidades nuevas o aumentadas puedan permitir que las amenazas exploten tales vulnerabilidades nuevas o con cambios.
- Vulnerabilidades identificadas para determinar aquellas que se exponen amenazas nuevas o que vuelven a emerger.
- El impacto aumentado o las consecuencias de las amenazas evaluadas, las vulnerabilidades y los riesgos en conjunto que dan como resultado un nivel inaceptable de riesgo.
- Incidentes de la seguridad de la información.

5.2.10 Monitoreo, revisión y mejora de la gestión del riesgo. El proceso de gestión del riesgo se deberá monitorear, revisar y mejorar continuamente, según sea necesario y adecuado; se debe verificar con regularidad que los criterios utilizados para medir el riesgo aún son válidos y consistentes con los objetivos, las estrategias y las políticas del negocio, y que los cambios en el contexto del negocio se toman en consideración de manera adecuada durante el proceso de gestión del riesgo, esta actividad debería abordar los siguientes aspectos como mínimo:

- Contexto legal y ambiental.
- Contexto de competición.
- Enfoque para la evaluación del riesgo.
- Categorías y valor de los activos.
- Criterios del impacto.
- Criterios de evaluación del riesgo.
- Criterios de aceptación del riesgo.
- Costo total de la propiedad.

5.3 SISTEMA DE CALIFICACIÓN DE VULNERABILIDADES

Las áreas de gestión de TI buscan identificar y evaluar vulnerabilidades a través de plataformas de hardware y software, para lograr esto requieren asignarles una prioridad y remediar de forma inmediata aquellas cuya evaluación genera un mayor riesgo para la organización.

El Common Vulnerability Scoring System (CVSS) proporciona un marco de referencia para comunicar características e impacto de las vulnerabilidades del área de TI. [19] CVSS está bajo la custodia del Foro de respuesta a Incidentes y equipo de Seguridad (FIRST)[20], sin embargo es un estándar abierto y libre.

[19] MELL, Peter; SCARFONE, Karen, National Institute of Standards and Technology y ROMANOSKY, Sasha. Carnegie Mellon University A Complete Guide to the Common Vulnerability Scoring System Version 2.0. [en línea]. CVSS, June 2007. Disponible en internet: URL< https://www.first.org/cvss/cvss-v2-guide.pdf>

[20] www.first.org/cvss

Aunque existen otros sistemas de puntuación de organizaciones comerciales y no comerciales cada uno de ellos maneja su propia métrica pero se diferencian el uno del otro por la evaluación y medida de las características de la vulnerabilidad, algunos ejemplos son:

- CERT/CC evalúa las vulnerabilidades en una escala de 0 a 180 desde el punto de vista del riesgo de la infraestructura de Internet.
- SANS toma en consideración si la vulnerabilidad es una debilidad de las Configuraciones por defecto o de sistemas cliente o servidor.
- Microsoft refleja la dificultad existente para lograr la explotación de la vulnerabilidad y el impacto en general.

Sin embargo, todos los anteriores sistemas aunque tienen un enfoque único para todas las vulnerabilidades asumen que el impacto de la materialización de una vulnerabilidad es constante y similar para cada organización.

El valor agregado al utilizar como guía el CVSS para determinar la criticidad de una vulnerabilidad son las métricas opcionales que provee el CVSS, métricas que evalúan los cambios en el tiempo que puedan tener las vulnerabilidades y los atributos propios del entorno del cliente donde aplica la vulnerabilidad.

Algunos de los beneficios del CVSS se exponen a continuación:

- Puntuaciones estandarizadas de Vulnerabilidad: Cuando una organización normaliza la puntuación de vulnerabilidad en todas las plataformas de software y hardware es posible implementar una sola política de administración de vulnerabilidades.
- Marco de referencia abierto: Las características utilizadas para obtener la puntuación de forma individual para cada vulnerabilidad son abiertas y libremente accesibles por lo que no se genera motivos para confusión.
- Priorización de riesgo: La puntuación calculada con los parámetros de entorno hace que la vulnerabilidad evaluada se trate de forma contextual. Lo cual quiere decir que las vulnerabilidades con esta puntuación miden el riesgo que la organización puede aceptar y/o mitigar.

Existen tres grupos de métricas usados por el CVSS para realizar la evaluación de las vulnerabilidades y cada uno maneja su propio conjunto de métricas, cuyo

propósito es definir y comunicar las características fundamentales de una vulnerabilidad[21]:

- Métrica Base: Representa las características fundamentales de una vulnerabilidad que es constante en el tiempo y en el entorno de usuario.
- Métrica Temporal: Representa los cambios en el tiempo de las característica de una vulnerabilidad pero no en el entorno de usuario.
- Métrica de Entorno: Representa las características relevantes y únicas de una vulnerabilidad para un entorno de usuario en particular y específico.

Las métricas proporcionan una representación clara de la vulnerabilidad. Las métricas temporal y de entorno son medidas complementarias que puede ser utilizadas con el fin de dar un contexto de la vulnerabilidad y precisar el riesgo que es único para un entorno determinado, lo cual permite tomar decisiones a la hora de mitigar los riesgos asociados a una vulnerabilidad.

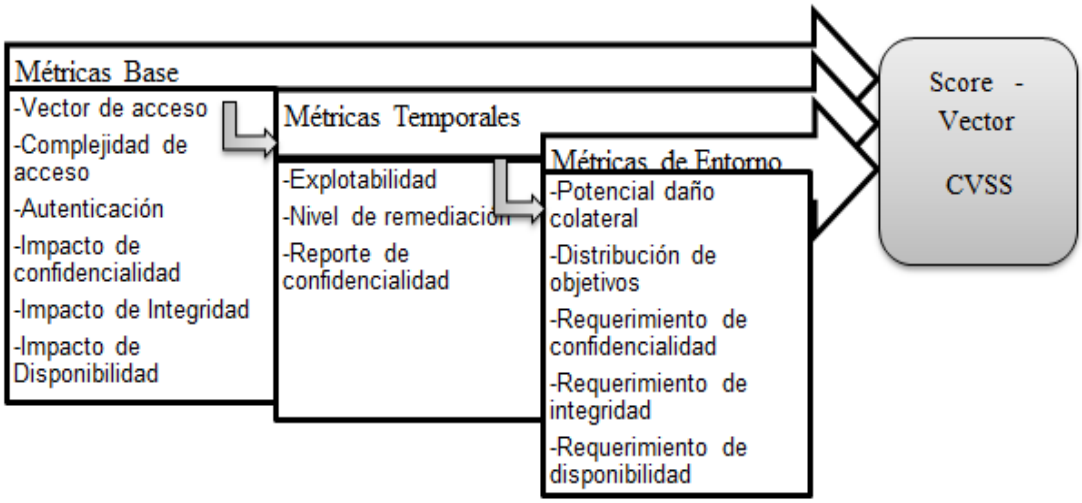
La puntuación inicial dada por el CVSS es establecida a partir de la Métricas Base que como resultado arroja un score (entre 0 y 10) y un vector que incluye los valores que fueron dados a la vulnerabilidad respecto a métricas de explotación y niveles de impacto, el vector provee información de cómo se deriva la puntuación de cada vulnerabilidad.

La puntuación de la Métrica Temporal es el resultado de su propia puntuación y la puntuación obtenida de la Métrica Base y de igual forma para obtener la puntuación de la Métrica de Entorno se basa en la puntuación de la Métrica Base y determina su propia puntuación.

La puntuación de cada Métrica es un valor entre 0 y 10 con los cuales se calcula un valor Overall que corresponde a la Métrica que posea mayor peso de las Métricas evaluadas. A continuación en la Figura 3 se muestran las métricas que se evalúan en cada grupo:

[21] MELL, Peter; SCARFONE, Karen, National Institute of Standards and Technology y ROMANOSKY, Sasha. Carnegie Mellon University A Complete Guide to the Common Vulnerability Scoring System Version 2.0. [en línea]. CVSS, June 2007. Disponible en internet: URL< https://www.first.org/cvss/cvss-v2-guide.pdf>

Figura 3 Métricas CVSS



Fuente: Autores Ana María Sossa López y Harvey Enrique Melo León

Para la métrica Base el de score lo ayudan a determinar la información encontrada en los boletines de análisis de vulnerabilidades, vendedores de aplicaciones o productos de seguridad, sin embargo para las otras métricas Temporal y de Entorno el valor de score lo determina solamente el usuario respecto a su propio entorno.

Existen diversas áreas que hacen uso del CVSS como por ejemplo:

- Proveedores de boletines de vulnerabilidades incluyen información de fecha en la que fue descubierta la vulnerabilidad, sistemas afectados y links de los vendedores donde están disponibles los parches para su remediación.
- Vendedores de aplicaciones de Software proveen la puntuación base y el vector del CVSS, esto ayuda para que se comunique la severidad de las vulnerabilidades para sus propios productos lo que hace que se maneje el riesgo de forma efectiva.
- Organizaciones privadas usan el CVSS de forma interna para tomar decisiones de administración de vulnerabilidades, usan la combinación de métricas de base, temporal y de entorno para obtener una evaluación contextual del riesgo y tomar acciones sobre aquellas que el riesgo sea mayor en sus sistemas.
- Administradores de seguridad (riesgo) usan la puntuación que provee el CVSS para calcular el riesgo de una organización o nivel de amenaza. Suelen utilizar aplicaciones desarrolladas específicamente para integrar la topología de red de la organización, datos de las vulnerabilidades, bases de datos de los equipos lo cual como resultado del análisis informa del nivel de riesgo asociado.
- Investigadores usan el CVSS para realizar análisis de estadísticas referente a las vulnerabilidades y sus aplicaciones.

A continuación se describen cada una de las métricas evaluadas en cada grupo y la definición de cada uno de los valores asignados:

5.3.1 Métrica Base. Las variables y métricas evaluadas en la métrica Base, permiten inferir como la vulnerabilidad es accedida y si son requeridas condiciones específicas para ser explotada. Las métricas que evalúan el impacto respecto a la confidencialidad, integridad y disponibilidad, miden la afectación directa a un activo de TI si la vulnerabilidad llega a ser explotada.

Vector de Acceso (AV)

Refleja como la vulnerabilidad es explotada. Cuanto más remoto un hacker puede acceder a un host para atacarlo mayor será la puntuación de la vulnerabilidad en esta métrica.

Los valores para medir esta métrica son:

Local (L): Si el intruso tiene acceso físico al sistema vulnerable o a la consola de administración. Ej., escalar privilegios de forma local.

Red adyacente (A): Si el atacante ya sea mediante un dominio de broadcast o colisión consigue el acceso al software vulnerable. Ej. Red de la ip local, Bluetooth.

Red (N): Significa que el software vulnerable está unido al stack de redes, el atacante no requiere acceso a la red o local. Ej., RPC buffer overflow.

Complejidad de acceso (AC)

Una vez el atacante ha ganado acceso al sistema objetivo se requiere saber que tan complejo es explotar la vulnerabilidad en el sistema. Depende la vulnerabilidad el atacante requerirá uno o varios pasos para conseguir explotarla. A menor complejidad mayor es la puntuación en esta métrica.

Los valores para medir la métrica son:

Alto (H): Cuando el sistema vulnerable posee condiciones de acceso especializadas.

Medio (M): Cuando las condiciones de acceso son algo especializadas. Ej.: La parte atacante es limitada a un grupo específico de usuarios o sistemas con algún nivel de autorización (posiblemente no confiables). Algún tipo de información debe ser garantizada antes de que un ataque exitoso pueda ser enviado. El atacante requiere aplicar un poco de ingeniería social para engañar e incautar la información de los usuarios.

Bajo (L): No existen condiciones de acceso especializadas. Ej. Requiere acceso a un rango de sistemas o usuarios posiblemente anónimos o no confiables. La configuración afectada es predeterminada.

Autenticación (Au)

Mide el número de veces que un atacante debe autenticarse con el objetivo para explotar la vulnerabilidad. Esta métrica no mide la complejidad del proceso de autenticación solamente evalúa que el atacante requiera credenciales antes de explotar la vulnerabilidad. A menor número de autenticaciones requeridas más alto es el puntaje de la vulnerabilidad.

Los valores para medir la métrica son:

Múltiple (M): Aplica cuando se requiere que la autenticación de un atacante sea dos o más veces incluso si se utilizan las mismas credenciales Ej. Aparte de requerir las credenciales para al sistema operativo se requiere las credenciales para acceso a la aplicación o la base de datos, etc.

Único (S): Un solo proceso de autenticación es requerido para conseguir el acceso para explotar la vulnerabilidad.

Ninguno (N): La autenticación no es requerida para acceder y explotar la vulnerabilidad.

Impacto de confidencialidad (C)

Con esta variable se mide el impacto en la confidencialidad al explotar una vulnerabilidad, entendiendo confidencialidad como limitar el acceso de la información o divulgación a los usuarios autorizados.

Los valores para medir la métrica son:

Ninguno (N): Cuando la explotación de la vulnerabilidad no genera impacto en la confidencialidad del sistema.

Parcial (P): Cuando existe una divulgación de información de forma considerable. Ej., cuando una vulnerabilidad divulga solamente ciertas tablas de la base de datos.

Completo (C): Cuando se ha divulgado totalmente información. El atacante puede leer toda la data de los sistemas.

Impacto de Integridad (I):

Esta variable mide el impacto en la integridad al explotar una vulnerabilidad. La integridad se refiere a la fiabilidad y garantía de la veracidad de la información.

Los valores para medir la métrica son:

Ninguno(N): No hay impacto en la integridad del sistema.

Parcial (P): Aplica para cuando existe modificación a algunos archivos del sistema o información, pero el atacante puede hacer modificaciones de forma limitada.

Completo (C): Aplica cuando existe compromiso total a la integridad del sistema. Hay una completa perdida de la protección del sistema.

Impacto de disponibilidad (A)

Mide el impacto causado a la disponibilidad luego de una explotación exitosa de la vulnerabilidad. La disponibilidad se refiere a la accesibilidad a los recursos de información. Ej., consumen de ancho de banda, espacio en disco.

Los valores para medir la métrica son:

Ninguno (N): No hay impacto en la disponibilidad del sistema.

Parcial (P): Aplica cuando existe reducción del rendimiento de un sistema.

Completo (C): Existe cuando hay un apagado total del recurso afectado. El atacante puede hacer que el recurso quede totalmente indisponible.

5.3.2 Métrica Temporal. La amenaza que representa una vulnerabilidad puede cambiar con el tiempo. La métrica temporal se basa en los siguientes factores:

- Confirmación del detalle técnico de la vulnerabilidad
- Estado de la remediación de la vulnerabilidad
- La disponibilidad de las técnicas o códigos de exploit.

Esta métrica es opcional y su uso dependerá si los usuarios deciden si aplica o no.

Explotabilidad

Mide el estado actual de las técnicas de exploit o la disponibilidad del código. Cuando el código del exploit se encuentra disponible públicamente, es de fácil acceso, por lo que se incrementa el número de atacantes potenciales no capacitados aumentando la severidad de la vulnerabilidad. Entre más fácil sea explotar la vulnerabilidad, más alto la puntuación en esta métrica.

Los valores para medir la métrica son:

No probado (U): El código del exploit no se encuentra disponible.

Prueba de concepto (POC): El código del exploit de una prueba de concepto requiere de modificaciones sustanciales por un atacante experto para que funcione en un ambiente específico.

Funcionalidad (F): El código del exploit está disponible.

Alto (H): Los detalles del código están totalmente disponibles y puede ser entregado por un agente de forma autónoma ya sea por un gusano o virus.

No definido (ND): Asignar esta variable no afecta la puntuación de este métrica, solo es informativa de forma que la ecuación no la utiliza.

Nivel de remediación (RL)

Esta métrica ayuda a medir el factor de priorización de la vulnerabilidad. Una vulnerabilidad típica es un parche no aplicado cuando recién se ha hecho la

publicación. Se propone ofrecer remediaciones provisionales mientras que oficialmente se instala el parche o actualiza la versión del software. Las etapas de remediación consideradas para este tipo de vulnerabilidades hacen que la puntuación disminuya en el tiempo, reduciendo así la urgencia a medida que la remediación se finaliza y la vulnerabilidad haya sido complemente subsanable.

Los valores para medir la métrica son:

Fix Oficial (OF): Cada vendedor ha sacado un parche oficial o una actualización del software.

Fix Temporal (TF): Existe un fix oficial pero solo está disponible temporalmente.

Solución alternativa (W): No hay una solución oficial por parte del vendedor. Para este caso algunos usuarios deben crearse su propio fix para remediar la vulnerabilidad.

No disponible (U): No hay solución disponible.

No definido (ND): Asignar esta variable no afecta la puntuación de este métrica, solo es informativa de forma que la ecuación no la utiliza.

Reporte de confidencia (RC)

Mide el grado de confidencialidad existente de la vulnerabilidad, la credibilidad y conocimiento en los detalles técnicos. En algunos casos, la existencia de las vulnerabilidades solo son publicadas pero sin detalles técnicos específicos, estas vulnerabilidades luego terminan siendo confirmadas por el conocimiento de los vendedores de la tecnología afectada. Cuanto más sea una vulnerabilidad validada por el vendedor, mayor será su puntuación.

Los valores para medir la métrica son:

No confirmada (UC): Existe una única fuente no confirmada. Hay muy poca confianza en la validez de los reportes.

No corroborada (UR): Existen múltiples fuentes no oficiales, como organizaciones de investigación o compañías de seguridad independientes.

Confirmada (C): La vulnerabilidad es de conocimiento por los vendedores de la tecnología afectada.

No definida (ND): Asignar esta variable no afecta la puntuación de este métrica, solo es informativa de forma que la ecuación no la utiliza.

5.3.3 Métricas de Entorno. Diferentes ambientes pueden tener un inmenso soporte del riesgo que implica la vulnerabilidad en la empresa u organización. Esta métrica captura las características de las vulnerabilidades asociado con el entorno de TI del usuario. Esta métrica es para uso de los usuarios quienes deciden si aplica o no.

Potencial daño colateral (CDP)

Esta métrica mide el daño potencial de la pérdida de vidas o activos físicos por daños o robos de propiedad o equipo. También mide económicamente la perdida de la productividad o ingresos. A mayor daño potencial mayor puntuación para la vulnerabilidad.

Los valores para medir la métrica son:

Ninguno (N): No hay pérdida potencial de vida, activos físicos, productividad o ingresos.

Bajo (L): Una explotación exitosa de la vulnerabilidad resulta en leves daños físicos o en la propiedad, de igual forma en la economía leves pérdidas en la productividad e ingresos.

Bajo-Medio (LM): Una explotación exitosa de la vulnerabilidad resulta en moderados daños físicos o en la propiedad y para la economía moderadas pérdidas en la productividad e ingresos.

Medio-Alto (MH): Una explotación exitosa de la vulnerabilidad resulta en significativos daños físicos o en la propiedad y para la economía significativas pérdidas en la productividad e ingresos.

Alta (H): Una explotación exitosa de la vulnerabilidad resulta en catastróficos daños físicos o en la propiedad y para la economía catastróficas pérdidas en la productividad e ingresos.

No definida (ND): Asignar esta variable no afecta la puntuación de este métrica, solo es informativa de forma que la ecuación no la utiliza.

Nota: Las organizaciones deben determinar la medida para asociar los daños y pérdidas de forma: leve, moderado, significativo o catastrófico.

Distribución de Objetivos (TD)

Mide la proporción de los sistemas vulnerables. Es un indicador específico del entorno para aproximar el porcentaje de sistemas que pueden ser afectados por una vulnerabilidad. A mayor proporción de sistemas vulnerables mayor la puntuación.

Los valores para medir la métrica son:

Ninguno (N): No existen sistemas objetivos. 0% de entorno en riesgo.

Bajo (L): Existen muy pocos objetivos en el entorno. Entre 1% - 25% del total está en riesgo.

Medio (M): Existen objetivos en el entorno en una escala media. Entre 26% - 75% del total está en riesgo.

Alto (H): Existen de forma considerable muchos objetivos en el entorno Entre 76% - 100% del total está en riesgo.

No definido (ND): Asignar esta variable no afecta la puntuación de este métrica, solo es informativa de forma que la ecuación no la utiliza.

Requerimiento de Seguridad (CR, IR, AR)

Esta métrica permite el análisis personalizado de la puntuación del CVSS dependiendo de la importancia del activo de TI afectado para los usuarios de una organización en términos de confidencialidad, integridad y disponibilidad. Cada factor de seguridad tiene tres posibles medidas: Bajo, Medio o Alto. A mayor requerimiento de seguridad, más alto el valor de la puntuación.

Los valores para medir la métrica son los mismos para los tres factores de seguridad:

Bajo (L): Pérdida de (Confidencialidad, Integridad, Disponibilidad) con posibilidades de tener efectos desfavorables de forma limitada en la organización.

Medio (M): Pérdida de (Confidencialidad, Integridad, Disponibilidad) con posibilidades de tener efectos desfavorables de forma seria en la organización.

Alto (H): Pérdida de (Confidencialidad, Integridad, Disponibilidad) con posibilidades de tener efectos desfavorables de forma catastrófica en la organización.

No definido (ND): Asignar esta variable no afecta la puntuación de este métrica, solo es informativa de forma que la ecuación no la utiliza.

6. INGENIERÍA DEL PROYECTO

En el presente capítulo se describe de forma detallada el estado del arte, los requerimientos, incluyendo a su vez el estudio de las diferentes variables de ingeniería que intervienen y los procesos para el desarrollo del plan de remediación propuesto.

6.1 ESTADO DEL ARTE

En la entidad bancaria las pruebas de intrusión son realizadas por una empresa de seguridad externa la cual se especializa en la identificación y explotación de vulnerabilidades y/o debilidades de seguridad en los componentes de infraestructura tecnológicos; las pruebas tienen como objetivo validar el estado de seguridad de los componentes de infraestructura críticos de la entidad, por lo cual la prueba de intrusión se realiza a un número determinado de activos de información, que para el caso de esta investigación es el equivalente 98 Activos de Información.

Los hallazgos identificados en la prueba son reportados a la Vicepresidencia de Operaciones y Tecnología a través de un memorando emitido por Contraloría General del Banco, esté contiene el detalle técnico de las pruebas realizadas, los hallazgos, vulnerabilidades, debilidades y recomendaciones dadas por el Proveedor encargado de realizar las pruebas.

De acuerdo con la política de Seguridad del Banco, la Vicepresidencia de Operaciones y Tecnología debe dar respuesta a la contraloría en un tiempo no mayor a 30 días respecto a en qué fecha se implementará la solución dada por el Proveedor para mitigar los riesgos identificados y materializados en la prueba.

6.2 REQUERIMIENTOS DE DISEÑO

En el desarrollo de este proyecto se enumeran los componentes que se necesitan para el progreso de esta investigación, cada uno de estos componentes son de vital importancia para la elaboración del plan de remediación de las vulnerabilidades cumpliendo así los objetivos del trabajo, estos componentes están clasificados según sus aspectos funcionales, técnicos y de seguridad:

6.2.1 Funcionales. A continuación se detallan los aspectos funcionales a considerar en el desarrollo de los objetivos del presente proyecto.

- Los controles y/o configuraciones a implementar en los componentes de infraestructura tecnológica del Banco para remediar las vulnerabilidades críticas no deben afectar la normal operación del Banco.
- Los procesos tecnológicos y/o operativos que se vean impactados por la implementación de las remediciones deben ser modificados y probados antes de su implementación en producción.
- Evitar la implementación de controles innecesarios que obstaculicen la normal operación del Banco.

6.2.2 Técnicos. A continuación se detallan los aspectos técnicos a considerar en el desarrollo de los objetivos del presente proyecto.

- Los controles a implementar sobre los componentes de infraestructura tecnológica deben ser aprobados por el Vicepresidente de Operaciones y Tecnología, Gerencia de Infraestructura, Gerencia de Telemática, Gerencia de Desarrollo y la Dirección de Seguridad Informática.
- Los controles técnicos a implementar deben ser validados desde el punto de vista de compatibilidad tecnológica, aplicabilidad operativa, aplicabilidad funcional y técnica;
- Deben ser validados por el especialista del componente de infraestructura de TI afectado para validar la factibilidad técnica de la implantación.

- La implementación de las remediaciones o controles deben ser programadas en las fechas establecidas como días hábiles para implementación de cambios en infraestructura tecnológica y en despliegue de Software.
- Aquellas remediaciones que correspondan a implementación de nuevas soluciones de seguridad, cambio en el Software desarrollado por el Banco y/o cambios significativos en la arquitectura de los componentes de infraestructura tecnológica deben ser trabajados como proyectos con todas las disposiciones establecidas por la Dirección de PMO del Banco.
- Todo control o herramienta de seguridad implementada debe ser licenciado y tener soporte.

6.2.3 Seguridad. A continuación se detallan los aspectos de seguridad a considerar en el desarrollo de los objetivos del presente proyecto.

- Calcular el Scoring real de las vulnerabilidades reportadas por el Proveedor, teniendo cuenta las métricas Base, Temporal y de ambiente especificadas en el framework Common Vulnerability Scoring System V2.0 (CVSS por sus siglas en ingles).
- Realizar la valoración del Riesgo haciendo uso de la metodología dada por la norma ISO 27005.
- Priorizar la remediación de vulnerabilidades.
- Definir los controles aplicables para mitigar, o llevar a un nivel aceptable los riesgos de Seguridad de la Información.

6.3 VARIABLES DE INGENIERÍA

Para la remediación de las Vulnerabilidades críticas, se tuvieron en cuenta una serie de variables de ingeniería, que intervinieron de manera directa en la ejecución de este trabajo, permitiendo el desarrollo y la conclusión del mismo, cada una de estas variables son analizadas de manera detallada para determinar su relevancia dentro de este objetivo.

6.3.1 Common Vulnerability Scoring System V2.0 (CVSS V2.0). Con el fin de establecer el nivel de afectación real que tiene cada vulnerabilidad reportada, se decidió utilizar la versión 2 del estándar Common Vulnerability Scoring System (CVSS V2 por sus siglas en ingles), ya que dicho estándar fue el empleado por la empresa de seguridad externa para medir y reportar el nivel de criticidad de las vulnerabilidades.

El método de calificación del CVSS relaciona las principales características de las vulnerabilidades, permitiendo generar una calificación numérica que indica la severidad o afectación de cada vulnerabilidad, esta valoración numérica es calculada a partir de criterios teóricos y prácticos definidos en el estándar en los siguientes tipos de métricas: métricas base, temporal y de entorno; a continuación en los cuadros 6, 7 y 8 se presentan las variables evaluadas en cada tipo de métrica:

Cuadro 6. Variables métrica base según CVSS 2.0

Categoría de la métrica	Métrica	Valor a asignar
Métricas de explotabilidad	Vector de acceso (AV)	Local (L)
		Red adyacente (A)
		Red (N)
	Complejidad de acceso (AC)	Alto (H)
		Medio (M)
		Bajo (L)
	Autenticación (Au)	Múltiple (M)
		Único (S)
		Ninguno (N)
Métricas de impacto	Impacto en la confidencialidad (C)	Ninguno (N)
		Parcial (P)
		Completo (C)
	Impacto en la integridad (I)	Ninguno (N)
		Parcial (P)
		Completo (C)
	Impacto en la disponibilidad (A)	Ninguno (N)
		Parcial (P)
		Completo (C)
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León		

Cuadro 7. Variables métrica temporal según CVSS 2.0

Métrica	Valor a asignar
Explotabilidad (E)	No definida (ND)
	No comprobado (U)
	Prueba de concepto (POC)
	Funcionalidad (F)
	Alto (H)
Nivel de remediación (RL)	No definida (ND)
	Fix oficial (OF)
	Fix temporal (TF)
	Solución alternativa (W)
	No disponible (U)
Reporte de confidencia (RC)	No definida (ND)
	No confinado (UC)
	No corroborado (UR)
	Confirmado (C)
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Cuadro 8. Variables métrica de entorno según CVSS 2.0

Categoría de la métrica	Métrica	Valor a asignar
Modificadores generales	Potencial daño colateral (CDP)	No definida (ND)
		Ninguno (N)
		Bajo (L)
		Medio - Bajo (LM)
		Medio - Alto (MH)
		Alto (H)
	Distribución de objetivo (TD)	No definida (ND)
		Ninguno 0% (N)
		Bajo 0%- 25 % (L)
		Medio 26% - 75% (M)
		Alto 76%-100% (H)
Modificadores de sub calificación de impacto	Requerimiento de confidencialidad (CR)	No definida (ND)
		Bajo (L)
		Medio (M)
		Alto (H)
	Requerimiento de	No definida (ND)

	integridad (IR)	Bajo (L)
		Medio (M)
		Alto (H)
	Requerimiento de disponibilidad (AR)	No definida (ND)
		Bajo (L)
		Medio (M)
		Alto (H)
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León		

6.3.2 Gestión del riesgo. En la elaboración del plan de remediación se pueden analizar las siguientes variables cualitativas para el cálculo del riesgo:

6.3.3 Probabilidad de ocurrencia del evento. La probabilidad de ocurrencia se mide en relación a que tan frecuente es la materialización de una amenaza determinada, en la tabla 3 se presenta el modelo de medición de la probabilidad:

Tabla 3. Probabilidad de Ocurrencia

Valor	Frecuencia	Criterio
Alto	Muy frecuente	Cuando ha ocurrido más de 4 veces en año
Medio	Frecuente	Entre 2 y 4 veces en el año.
Bajo	Poco frecuente	Una vez cada 5 años
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León		

6.3.4 Cálculo impacto. El impacto corresponde a la medida del daño ocasionado sobre un activo de información como consecuencia de la materialización de una amenaza. Conociendo la importancia del activo y la afectación que causan las amenazas, es posible determinar el impacto, en la tabla 4 se muestra la clasificación del impacto:

Tabla 4. Clasificación del impacto

Impacto	
Alto	Impacto alto
Medio	Impacto medio
Bajo	Impacto bajo
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

El cuadro 9 corresponde la medición de impacto:

Cuadro 9. Medición de impacto

Impacto		Afectación de la vulnerabilidad en el activo de Información		
		Bajo	Medio	Alto
Importancia del activo de información	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Donde para esta investigación las variables a determinar son la afectación de cada Amenaza y/o vulnerabilidad reportada.

6.3.5 Cálculo del riesgo. Es posible calcular el riesgo conociendo el impacto que tiene la materialización de una amenaza versus la probabilidad de que se materialice la misma, a continuación en la tabla 5 se muestra la clasificación del riesgo:

Tabla 5. Clasificación del riesgo

Riesgo	
Alto	Riesgo alto
Medio	Riesgo medio

Bajo	Riesgo bajo
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

En el cuadro 10 presenta la definición del modelo de medición del riesgo:

Cuadro 10. Medición del Riesgo

Riesgo		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

6.3.6 Tratamiento del riesgo. Para cada riesgo Alto se debe determinar el tipo de tratamiento de riesgo según las siguientes consideraciones:

- Reducción del Riesgo: Implementación de controles que reduzcan el riesgo a niveles aceptables. Los niveles de riesgos aceptables son definidos mediante el cálculo de riesgo residual y la definición de aceptación de riesgo.
- Retención del Riesgo: No realizar ninguna acción según el resultado del análisis de riesgo residual y los criterios de aceptación de riesgo definidos.
- Transferencia de riesgos: Transferir el riesgo a otra de las partes que pueda manejar el riesgo de manera más eficaz.
- Evasión del Riesgo: Eliminación del proceso, Componente de TI y/o activo de información, cambio de arquitectura de la solución afectada, o cambio de tecnología.

6.3.6.1 Cálculo riesgo residual. Para calcular el riesgo residual se deben tener en cuentas las siguientes variables:

- La relación entre valor cualitativo y cuantitativo del riesgo calculado, a continuación en la tabla 6 se presenta esta relación:

Tabla 6. Relación entre valor cualitativo y cuantitativo del Riesgo

Riesgo calculado	Valor cuantitativo
Alto	3
Medio	2
Bajo	1
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

- La relación entre el valor cualitativo y cuantitativo de la efectividad de los controles establecidos para mitigar los riesgos, a continuación en la tabla 7 muestra esta relación:

Tabla 7. Relación entre el valor cualitativo y cuantitativo de la efectividad de los controles

Efectividad del control	Valor cuantitativo
Bajo	1
Medio	2
Alto	3
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

- Riesgo residual. Se definió riesgo residual como la diferencia que existe entre el riesgo calculado y la efectividad de los controles implementados para reducir el riesgo; la fórmula matemática es detallada en la ecuación 1:

Ecuación 1. Formula Determinación del riesgo residual

$$RiesgoResidual = RiesgoCalculado - \overline{X}EfectividadControles$$

Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León

6.3.6.2 Aceptación del riesgo residual. Los criterios de aceptación de riesgo fueron definidos de acuerdo con los criterios presentados en la tabla 8:

Tabla 8. Criterios de aceptación del riesgo

Nivel de riesgo residual	Criterio de aceptación	Descripción
0 >= y =< 1	Aceptable	Reducción del riesgo Eliminación del riesgo Evasión del riesgo Transferencia del riesgo
1 >= y =< 2	No Aceptable	N/A
2 >= y =< 3	No Aceptable	N/A
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León		

7. DESARROLLO DEL PROYECTO

En esta sección del documento final se muestra el procedimiento que se realizó para alcanzar los objetivos propuestos.

Para la elaboración del plan de remediación de las vulnerabilidades críticas se desarrolló la siguiente metodología:

- Estimación del riesgo para determinar la criticidad de las vulnerabilidades.
- Determinar los controles y/o configuraciones que se deben implementar para mitigar el riesgo o que como resultado de su implementación permitan disminuir a un nivel aceptable el riesgo para las vulnerabilidades críticas.
- Definición de los tiempos de remediación de las Vulnerabilidades según el nivel de riesgo.
- Elaboración del plan de trabajo para la remediación de las vulnerabilidades críticas.
- Aprobación del plan de trabajo.

7.1 ESTIMACIÓN DEL RIESGO

7.1.1 Identificación de la importancia de los activos de información atacados. En el caso de la entidad bancaria la clasificación de los activos de información esta implementada desde el año 2010 de acuerdo con los parámetros de la política interna XXX-XXX-XX-001, a continuación en la tabla 9 se presenta la clasificación de los activos de información atacados en la prueba de intrusión:

Tabla 9. Clasificación activos de información

Dirección IP	Nombre servidor	Finalidad de negocio	Criticidad
x.x.x.x	server	Controladores de domino	Alta
x.x.x.x	server	Aplicación vinculación del clientes	Alta
550 Activos	PC'S	Estación de trabajo personal	Baja

Tabla 9. (Continuación)

Dirección IP	Nombre servidor	Finalidad de negocio	Criticidad
x.x.x.x	server	Aplicación de tesorería	Media
x.x.x.x	server	Servidor de intercambio de información TI	Meda
x.x.x.x	server	Servidor de aplicación de crédito	Alta
x.x.x.x	server	Controladores de domino	Alta
x.x.x.x	server	Controladores de domino	Alta
x.x.x.x	server	Aplicación de Onbase (documentación clientes)	Alta
x.x.x.x	server	Servidor de intercambio entre DB-User	Media
x.x.x.x	Server	Aplicación de recursos humanos	Media
x.x.x.x	Server	Filtro de contenido WEB	Alta
x.x.x.x	SERVER	Firewall de NAC	Alta
N/A	Cuentas del Dominio de la organización	No es un activo de información del banco	N/A
x.x.x.x	Server	Servidor web service porvenir	Medio
x.x.x.x	PC	Estación de trabajo personal	Baja
x.x.x.x	PC	Estación de trabajo personal	Baja
500 Activos	Desktop's	Estación de trabajo personal	Baja
x.x.x.x	Server	Administración nómina	Alta
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León			

7.1.2 Identificación de amenazas. En el informe de pruebas de intrusión no se establecen las amenazas empleadas en la prueba y debido a que éstas son fundamentales en la estimación del riesgo, se definió la estrategia que se presenta en este subcapítulo para poder determinarlas, a continuación en la tabla 10 se presentan las vulnerabilidades reportadas por el proveedor:

Tabla 10. Vulnerabilidades detectadas en la prueba de Intrusión

IP afectadas	Nombre servidor	Criticidad proveedor	Vulnerabilidades
x.x.x.x	server	Alta	Infección de servidor
x.x.x.x	server	Alta	Vulnerabilidad Volcado de contenido de memoria RAM-Obtención Tickets de Kerberos válidos
x.x.x.x	server	Alta	Volcado de memoria RAM a través de programas ejecutados a través de RDP-compartir recursos locales

Tabla 10. (Continuación)

IP afectadas	Nombre servidor	Criticidad proveedor	Vulnerabilidades
x.x.x.x	server	Alta	Versión de Oracle Database obsoleta
550 Activos	PC'S	Alta	Acceso BIOS sin contraseña
550 Activos	PC'S	Alta	Arranque de equipo de escritorio con otro sistema operativo
x.x.x.x	server	Alta	Versión de Microsoft Windows Server 2003 obsoleta
x.x.x.x	server	Alta	Sesiones CIFS NULL permitidas
x.x.x.x	server	Alta	Sesiones CIFS NULL permitidas
x.x.x.x	server	Alta	Sesiones CIFS NULL permitidas
x.x.x.x	server	Alta	Sesiones CIFS NULL permitidas
x.x.x.x	server	Alta	Sesiones CIFS NULL permitidas
x.x.x.x	server	Alta	Sesiones CIFS NULL permitidas
x.x.x.x	server	Alta	Servicio VNC remote control service instalado
x.x.x.x	server	Media	Apache HTTPD: Range header remote DoS
x.x.x.x	server	Media	Apache HTTPD: Range header remote DoS
x.x.x.x	server	Media	SMB signing deshabilitado
x.x.x.x	server	Media	SMB signing deshabilitado
x.x.x.x	Server	Media	SMB signing deshabilitado
x.x.x.x	server	Media	SMB signing deshabilitado
x.x.x.x	Server	Media	Vulnerabilidad OpenSSL SSL/TLS MITM
x.x.x.x	Server	Media	Servidor TLS/SSL soporta SSLv2 y SSLv3
x.x.x.x	Server	Media	Certificado SSL invalido

x.x.x.x	Server	Media	Servidor TLS/SSL soporta algoritmos Cipher débiles
x.x.x.x	Server	Media	Cifrado RC4 en protocolo SSL
x.x.x.x:8443	SERVER	Media	Certificado SSL invalido
Cuentas del Dominio de la organización	Cuentas del Dominio de la organización	Alta	Contraseñas débiles
550 Activos	PC'S	Alta	1) Volcado de contenido de memoria RAM (local y remoto) 2) Obtención de credenciales almacenadas en procesos
x.x.x.x	Server	Alta	1) Volcado de contenido de memoria RAM (local y remoto) 2) Obtención de credenciales almacenadas en procesos

Tabla 10. (Continuación)

IP afectadas	Nombre servidor	criticidad	Vulnerabilidades
x.x.x.x	Server	Alta	1) Volcado de contenido de memoria RAM (local y remoto) 2) Obtención de credenciales almacenadas en procesos
x.x.x.x	PC	Alta	Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”
x.x.x.x	PC	Alta	Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”
550 Activos	PC'S	Alta	Escalada de privilegios mediante cuentas administradoras locales "XXXXX" "XXXXX" "XXX" "XXXXX" “XXXX"
550 Activos	PC'S	Alta	Escalada de Privilegios mediante cuenta administradora de dominio Usuario: "XXXX", "XXXXX", "inv"
x.x.x.x	Server	Alta	Múltiples vulnerabilidades en IBM WebSphere Application Server 6.1
x.x.x.x	Server	Medio	Microsoft Windows RDP Man in The Middle
500 Activos	Desktop's	Alta	Usuario administrador local sin contraseña
x.x.x.x	Server	Alta	Credenciales por defecto o fáciles de averiguar "Quest Software"
x.x.x.x	Server	Alta	Expansión de control sobre el sistema operativo desde la base de datos
x.x.x.x	Server	Alta	Transmisión de información sin cifrar
x.x.x.x	Server	Alta	Múltiples vulnerabilidades en Oracle Database Server

Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León

Con el fin de identificar las amenazas correspondientes a las vulnerabilidades reportadas, se definieron las siguientes categorías y tipos de amenaza como se muestra en el cuadro 11:

Cuadro 11. Categorías y tipos de amenazas.

Categoría de Amenaza	Tipo Amenaza
Compromiso de componentes de TI	Malware
	Explotación de vulnerabilidades de software
Software obsoleto	Vulneración de software obsoleto
Acceso no autorizado al componente de TI	Usuarios sin password
	Uso de password débiles
	Mala configuración de software
	Uso de password de industria
Compromiso de información	Información en texto claro
	Interceptación de tráfico
	Suplantación de certificado digital
	Uso de password de industria
	Uso de herramientas de Hacking

Denegación de Servicio	Explotación de vulnerabilidades de software
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Una vez definidos los tipos de amenazas, se procedió a asignar cada vulnerabilidad con su correspondiente amenaza como se muestra en la tabla 11:

Tabla 11. Clasificación tipos de amenazas

Activo de información	Criticidad dada x proveedor	Categoría amenaza	Tipo de amenaza	Vulnerabilidad proveedor	Vulnerabilidades
server	Alta	Compromiso de componentes de TI	Malware	Infección de servidor	Antivirus inexistente o mal configurado

Tabla 11. (Continuación)

Activo de información	Criticidad dada x proveedor	Categoría amenaza	Tipo de amenaza	Vulnerabilidad proveedor	Vulnerabilidades
server	Alta	Compromiso de información	Uso de herramientas de Hacking	Vulnerabilidad volcado de contenido de memoria RAM-obtención Tickets de Kerberos validos	Servidor sin fixes de seguridad
server	Alta	Compromiso de información	Uso de herramientas de Hacking	Volcado de memoria RAM a través de programas ejecutados a través de RDP-compartir recursos locales	Estaciones de trabajo mal configuradas.
server	Alta	Software obsoleto	Vulneración de software obsoleto	Versión de Oracle Database obsoleta	Servidor fuera de Soporte
PC'S	Alta	Acceso no autorizado al	Usuarios sin Password	Acceso BIOS sin contraseña	Falta de autenticación en la BIOS

		componente de TI			
PC'S	Alta	Compromiso de información	Uso de herramientas de Hacking	Arranque de equipo de escritorio con otro sistema operativo	Falta de autenticación en la BIOS
server	Alta	Software obsoleto	Vulneración de software obsoleto	Versión de Microsoft Windows Server 2003 obsoleta	Servidor fuera de Soporte
server	Alta	Compromiso de información	Uso de password de Industria	Sesiones CIFS NULL permitidas	Mala configuración en el servidor
server	Alta	Compromiso de información	Uso de password de Industria	Sesiones CIFS NULL permitidas	Mala configuración en el servidor
server	Alta	Compromiso de información	Uso de password de Industria	Sesiones CIFS NULL permitidas	Mala configuración en el servidor

Tabla 11. (Continuación)

Activo de información	Criticidad dada x proveedor	Categoría amenaza	Tipo de amenaza	Vulnerabilidad proveedor	Vulnerabilidades
server	Alta	Compromiso de información	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el servidor
server	Alta	Compromiso de información	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el servidor
server	Alta	Compromiso de información	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el servidor
server	Alta	Compromiso de información	Explotación de Vulnerabilidades de Software	Acceso no autorizado explotando vulnerabilidades del Servicio VNC remote control.	Software no autorizado instalado en el servidor
server	Alta	Compromiso de información	Explotación de vulnerabilidades de software	Acceso no autorizado explotando vulnerabilidades del Servicio VNC remote control.	Software no autorizado instalado en el servidor
server	Media	Denegación	Explotación de	Denegación de	Servidor sin fixes

		de Servicio	vulnerabilidades de software	servicio por vulnerabilidad: Apache HTTPD: Range header remote DoS.	de Seguridad
server	Media	Denegación de Servicio	Explotación de vulnerabilidades de software	Denegación de servicio por vulnerabilidad: Apache HTTPD: Range header remote DoS.	Servidor sin fixes de Seguridad
server	Media	Compromiso de información	Interceptación de tráfico	Suplantación de cuentas de usuario a través de SMB.	SMB signing deshabilitado
server	Media	Compromiso de información	Interceptación de tráfico	Suplantación de cuentas de usuario a través de SMB.	SMB signing deshabilitado
Server	Media	Compromiso de información	Interceptación de tráfico	Suplantación de ctas de usuarios a través de SMB.	SMB signing deshabilitado

Tabla 11. (Continuación)

Activo de información	Criticidad dada x proveedor	Categoría amenaza	Tipo de amenaza	Vulnerabilidad proveedor	Vulnerabilidades
server	Media	Compromiso de información	Interceptación de tráfico	Suplantación de cuentas de usuario a través de SMB.	SMB signing Deshabilitado
Server	Media	Compromiso de información	Interceptación de tráfico	Interceptación de tráfico por vulnerabilidad OpenSSL SSL/TLS MITM	Servidor sin Fixes de Seguridad
Server	Media	Compromiso de información	Interceptación de tráfico	Servidor TLS/SSL soporta SSLv2 y SSLv3	Mala Configuración en los servidores
Server	Media	Compromiso de información	Interceptación de tráfico	Interceptación de tráfico por suplantación de certificado	Certificado SSL invalido
Server	Media	Compromiso de información	Interceptación de tráfico	Interceptación de tráfico por algoritmos Cipher débiles servidor TLS/SSL	Mala Configuración en los servidores

Server	Media	Compromiso de información	Interceptación de tráfico	Interceptación de tráfico por cifrado RC4 en protocolo SSL	Mala Configuración en los servidores
SERVER	Media	Compromiso de información	Suplantación de certificado digital	Interceptación de tráfico por suplantación de certificado	Certificado SSL invalido
Cuentas del Dominio de la organización	Alta	Acceso no autorizado al componente de TI	Uso de password débiles	Acceso No autorizado por contraseñas débiles	Contraseñas débiles
PC'S	Alta	Compromiso de información	Uso de herramientas de Hacking	1) Volcado de contenido de memoria RAM (local y remoto) 2) Obtención de credenciales almacenadas en procesos	Estaciones de trabajo sin Fixes de seguridad

Tabla 11. (Continuación)

Activo de información	Criticidad dada x proveedor	Categoría amenaza	Tipo de amenaza	Vulnerabilidad proveedor	Vulnerabilidades
Server	Alta	Compromiso de información	Uso de herramientas de Hacking	1) Volcado de contenido de memoria RAM (local y remoto) 2) Obtención de credenciales almacenadas en procesos	Servidor sin Fixes de Seguridad
Server	Alta	Compromiso de información	Uso de herramientas de Hacking	1) Volcado de contenido de memoria RAM (local y remoto) 2) Obtención de credenciales almacenadas en procesos	Servidor sin Fixes de Seguridad
PC	Alta	Acceso no autorizado al componente de TI	Mala Configuración de Software	Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas	Mala Configuración en los PC

				especiales”	
PC	Alta	Acceso no autorizado al componente de TI	Mala Configuración de Software	Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”	Mala Configuración en los PC
PC'S	Alta	Acceso no autorizado al componente de TI	Mala Configuración de Software	Escalada de Privilegios mediante cuentas Administradoras Locales "XXXXX" "XXXXX" "XXX" "XXXXX" "XXXX"	Mala Configuración en los PC
PC'S	Alta	Acceso no autorizado al componente de TI	Mala Configuración de Software	Escalada de Privilegios mediante cuenta Administradora de Dominio Usuario: "XXXX", "XXXXX", "inv"	Mala Configuración en los PC

Tabla 11. (Continuación)

Activo de información	Criticidad dada x proveedor	Categoría amenaza	Tipo de amenaza	Vulnerabilidad proveedor	Vulnerabilidades
Server	Alta	Software Obsoleto	Vulneración de Software obsoleto	Múltiples vulnerabilidades en IBM WebSphere Application Server 6.1	Servidor Fuera de Soporte
Server	Medio	Compromiso de Información	Interceptación de tráfico	Interceptación de tráfico a través de Microsoft Windows RDP Man in The Middle	Servidor sin Fixes de Seguridad
Server	Medio	Compromiso de Información	Interceptación de tráfico	Interceptación de tráfico a través de Microsoft Windows RDP Man in The Middle Vulnerability	Servidor sin Fixes de Seguridad
Desktop's	Alta	Acceso no autorizado al componente de TI	Usuarios sin Password	Acceso no Autorizado al sistema por usuario administrador	Usuarios sin Passwords

				local sin contraseña	
Server	Alta	Acceso no autorizado al componente de TI	Uso de password de Industria	Credenciales por defecto o fáciles de averiguar "Quest Software"	Contraseñas por defecto
Server	Alta	Compromiso de componentes de TI	Explotación de Vulnerabilidades de Software	Control sobre el Sistema Operativo desde la Base de Datos	Servidor sin Fixes de Seguridad
Server	Alta	Compromiso de Información	Información en texto Claro	Transmisión de información sin cifrar	Falta de Mecanismos de Cifrado
Server	Alta	Compromiso de componentes de TI	Explotación de Vulnerabilidades de Software	Múltiples vulnerabilidades en Oracle Database Server	Servidor sin Fixes de Seguridad
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

7.1.3 Afectación de las amenazas en los activos de información. La severidad de las vulnerabilidades reportadas por el proveedor fueron determinadas con la metodología CVSSv2 a partir de la métrica base ya que esté no contaba con información como la criticidad de los activos de información, por esta razón en esta investigación se considera importante realizar el cálculo del scoring o criticidad de la vulnerabilidad aplicando las métricas base, temporal y de entorno definidas en la metodología CVSS v2.

7.1.3.1 Scoring vulnerabilidades CVSS V2. Para determinar la severidad de las vulnerabilidades se utilizó la clasificación cuantitativa-cualitativa de severidad empleada por la NVD (National Vulnerability Database)[22], la cual tiene tres niveles cualitativos relacionados con una escala cuantitativa de 0 a 10 como se muestra en la tabla 12:

Tabla 12. Calificaciones de la severidad de las vulnerabilidades

Severidad – NVD	Calificación - CVSS
Baja	0.0 – 3.9
Media	4.0 – 6.9

[22] National Vulnerability Database. [en línea]. Common Vulnerability Scoring System Version 2 Calculator. Disponible en Internet: URL<https://nvd.nist.gov/cvss.cfm?calculator&adv&version=2>

Alta	7.0 – 10.0
Fuente: NVD Vulnerability Severity Ratings. [En línea]. Disponible en: https://nvd.nist.gov/cvss.cfm	

Para obtener la severidad real de cada vulnerabilidad teniendo en cuenta el ambiente tecnológico de la entidad bancaria, se utilizó la herramienta de cálculo CVSSv2.0 online de la NIST disponible en la página web https://nvd.nist.gov/CVSS/v2-calculator; a continuación en la tabla 13 se presenta la calificación otorgada a cada vulnerabilidad respecto a la métrica base, temporal y de entorno, así como la calificación general (OVERALL) obtenida:

Tabla 13. Severidad de las vulnerabilidades aplicando las métricas Base, temporal y de entorno

Activo de información	Vulnerabilidad	Métrica base	Métrica temporal	Métrica entorno	Overall	Severidad del CVSS
server	Infección de Servidor	7,4	6,7	8,4	8,4	Alta
server	Vulnerabilidad Volcado de contenido de memoria RAM-Obtención Tickets de Kerberos Validos	7,9	7,5	5,2	5,2	Media
server	Volcado de memoria RAM a través de Programas ejecutados a través de RDP-compartir recursos locales.	7,9	7,5	8,9	8,9	Alta
server	Versión de Oracle Database obsoleta	8,5	7	7,9	7,9	Alta
PC'S	Acceso BIOS sin contraseña	7,2	8,1	8,1	8,1	Alta
PC'S	Arranque de equipo de escritorio con otro sistema operativo	7,2	8,1	8,1	8,1	Alta

server	Versión de Microsoft Windows server 2003 obsoleta	8,5	7,7	7,7	7,7	Alta
server	Sesiones CIFS NULL permitidas	7,5	5,9	6,1	6,1	Media
server	Sesiones CIFS NULL permitidas	7,5	5,9	6,1	6,1	Media
server	Sesiones CIFS NULL permitidas	7,5	5,9	6,1	6,1	Media
server	Sesiones CIFS NULL permitidas	7,5	5,9	6,1	6,1	Media
server	Sesiones CIFS NULL permitidas	7,5	5,9	6,1	6,1	Media

Tabla 13. (Continuación)

Activo de información	Vulnerabilidad	Métrica base	Métrica temporal	Métrica entorno	Overall	Severidad del CVSS
server	Sesiones CIFS NULL permitidas	7,5	5,9	6,1	6,1	Media
server	Acceso no autorizado explotando vulnerabilidades del servicio VNC remote control.	7,5	7,5	8,7	8,7	Alta
server	Denegación de servicio por vulnerabilidad: apache HTTPD: Range header remote DoS.	6,8	5,6	6,3	6,3	Media
server	Denegación de Servicio por vulnerabilidad: apache HTTPD: Range header remote DoS.	6,8	5,6	6,3	6,3	Media
server	Suplantación de cuentas de usuario a través de SMB.	6,8	5,8	5,9	5,9	Media
server	Suplantación de cuentas de usuario a través de SMB.	6,8	5,8	5,9	5,9	Media
Server	Suplantación de cuentas de	6,8	5,8	5,9	5,9	Media

	usuario a través de SMB.					
server	Suplantación de cuentas de usuario a través de SMB.	6,8	5,8	5,9	5,9	Media
Server	Interceptación de tráfico por vulnerabilidad OpenSSL SSL/TLS MITM	6,8	2,3	1,3	1,3	Baja
Server	Servidor TLS/SSL soporta SSLv2 y SSLv3	5,8	2,3	1,3	1,3	Baja
Server	Interceptación de tráfico por suplantación de certificado	5,8	3,1	4,5	4,5	Media

Tabla 13. (Continuación)

Activo de información	Vulnerabilidad	Métrica base	Métrica temporal	Métrica entorno	Overall	Severidad del CVSS
Server	Interceptación de tráfico por algoritmos Cipher débiles servidor TLS/SSL	5,8	2,3	1,3	1,3	Baja
Server	Interceptación de tráfico por cifrado RC4 en protocolo SSL	4,3	2,3	1,3	1,3	Baja
SERVER	Interceptación de tráfico por suplantación de certificado	5,8	3,1	4,5	4,5	Media
Cuentas del Dominio de la organización	Acceso no autorizado por contraseñas débiles	8,3	7,9	9	9	Alta
PC'S	1) Volcado de contenido de memoria RAM (local y remoto) 2) Obtención de credenciales almacenadas en procesos	7,9	7,9	8,5	8,5	Alta
Server	1) Volcado de contenido de memoria RAM (local y remoto)	7,9	7,9	8,5	8,5	Alta

	2) Obtención de credenciales almacenadas en procesos					
Server	1) Volcado de contenido de memoria RAM (local y remoto) 2) Obtención de credenciales almacenadas en procesos	7,9	7,9	8,5	8,5	Alta

Tabla 13. (Continuación)

Activo de información	Vulnerabilidad	Métrica base	Métrica temporal	Métrica entorno	Overall	Severidad del CVSS
PC	Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”	7,2	7,1	8,6	8,6	Alta
PC	Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”	7,2	7,1	8,6	8,6	Alta
PC'S	Escalada de privilegios mediante cuentas administradoras locales "XXXXX" "XXXXX" "XXX" "XXXXX" "XXXX"	7,2	7,9	9	9	Alta
PC'S	Escalada de privilegios mediante cuenta administradora de dominio usuario: "XXXX", "XXXXX", "inv"	7,7	7,9	9	9	Alta
Server	Múltiples vulnerabilidades en IBM WebSphere	7,7	6,4	7,8	7,8	Alta

	Application Server 6.1					
Server	Interceptación de tráfico a través de Microsoft Windows RDP Man in The Middle	4	3,6	6,9	6,9	Media
Server	Interceptación de tráfico a través de Microsoft Windows RDP Man in The Middle Vulnerability	4	3,6	6,9	6,9	Media
Desktop's	Acceso no autorizado al sistema por usuario administrador local sin contraseña	8,2	8,3	9,2	9,2	Alta

Tabla 13. (Continuación)

Activo de información	Vulnerabilidad	Métrica base	Métrica temporal	Métrica entorno	Overall	Severidad del CVSS
Server	Credenciales por defecto o fáciles de averiguar "Quest Software"	8,3	6,3	1,6	1,6	Baja
PC	Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”	7,2	7,1	8,6	8,6	Alta
Server	Control sobre el sistema operativo desde la Base de Datos	7,2	7,2	6,5	6,5	Media
Server	Transmisión de información sin cifrar	7,1	6,4	5,2	5,2	Media
Server	Múltiples vulnerabilidades en Oracle Database Server	7,7	6,4	8,2	8,2	Alta
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León						

Luego de calcular el nivel de severidad cada vulnerabilidad respecto a las métricas de base, tiempo y entorno, se obtiene como resultado final la calificación (Overall)

la cual acuerdo al rango establecido por el NVD indica el nivel de afectación por vulnerabilidad (Alto, medio, Bajo).

Este sub capitulo permitió determinar la afectación de las vulnerabilidades en cada activo de información, lo cual es un parámetro fundamental para determinar el Impacto.

7.1.3.2 Determinación del impacto. Según la definición de impacto establecida en el... Capítulo 6.3.4... para el cálculo del mismo, se requieren dos variables: la afectación de las amenazas que fue determinada en el ... Capítulo 7.1.3.1... y la criticidad de los activos que fue definida en el... Capítulo 7.1.1... ; en el … Anexo A… se detalla la matriz de determinación del impacto para cada vulnerabilidad.

A continuación en la tabla 14 se presenta el resultado del impacto de cada vulnerabilidad:

Tabla 14. Impacto de las vulnerabilidades

Activo de información	Impacto	Amenaza	Amenaza proveedor	Vulnerabilidades
server	Alto	Malware	Infección de servidor	Antivirus inexistente o mal configurado
server	Alto	Uso de herramientas de Hacking	Vulnerabilidad Volcado de contenido de memoria RAM-Obtención Tickets de Kerberos Validos	Servidor sin Fixes de seguridad
server	Alto	Uso de herramientas de Hacking	Volcado de memoria RAM a través de programas ejecutados a través de RDP-compartir recursos locales.	Estaciones de trabajo Mal configuradas.
server	Alto	Vulneración de software obsoleto	Versión de Oracle Database obsoleta	Servidor fuera de soporte
PC'S	Medio	Usuarios sin Password	Acceso BIOS sin contraseña	Falta de autenticación en la BIOS
PC'S	Medio	Uso de herramientas de Hacking	Arranque de equipo de escritorio con otro sistema operativo	Falta de autenticación en la BIOS
server	Alto	Vulneración de software obsoleto	Versión de Microsoft Windows server 2003	Servidor fuera de soporte

			obsoleta	
server	Medio	Uso de password de Industria	Sesiones CIFS NULL permitidas	Mala configuración en el servidor
server	Medio	Uso de password de Industria	Sesiones CIFS NULL permitidas	Mala configuración en el servidor

Tabla 14. (Continuación)

Activo de información	Impacto	Amenaza	Amenaza proveedor	Vulnerabilidades
server	Alto	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el servidor
server	Alto	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el servidor
server	Alto	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el servidor
server	Alto	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el servidor
server	Alto	Explotación de vulnerabilidades de software	Acceso no autorizado explotando vulnerabilidades del Servicio VNC remote control.	Software no autorizado instalado en el servidor
server	Alto	Explotación de vulnerabilidades de software	Denegación de servicio por vulnerabilidad: Apache HTTPD: Range header remote DoS.	Servidor sin Fixes de seguridad
server	Medio	Explotación de vulnerabilidades de software	Denegación de servicio por vulnerabilidad: Apache HTTPD: Range header remote DoS.	Servidor sin Fixes de seguridad
server	Medio	Interceptación de tráfico	Suplantación de cuentas de usuario a través de SMB.	SMB signing deshabilitado
server	Alto	Interceptación de tráfico	Suplantación de cuentas de usuario a través de SMB.	SMB signing deshabilitado
Server	Medio	Interceptación de tráfico	Suplantación de cuentas de usuario a través de SMB.	SMB signing deshabilitado
server	Medio	Interceptación de tráfico	Suplantación de cuentas de usuario a través de SMB.	SMB signing deshabilitado
Server	Medio	Interceptación de tráfico	Interceptación de tráfico por vulnerabilidad OpenSSL SSL/TLS MITM	Servidor sin Fixes de seguridad
Server	Medio	Interceptación de tráfico	Servidor TLS/SSL soporta SSLv2 y SSLv3	Mala configuración en el servidor
Server	Alto	Interceptación de tráfico	Interceptación de tráfico por suplantación de certificado	Certificado SSL invalido
Server	Medio	Interceptación de tráfico	Interceptación de tráfico por algoritmos Cipher débiles	Mala configuración en

			Servidor TLS/SSL	el servidor

Tabla 14. (Continuación)

Activo de información	Impacto	Amenaza	Amenaza proveedor	Vulnerabilidades
Server	Medio	Interceptación de tráfico	Interceptación de tráfico por Cifrado RC4 en protocolo SSL	Mala configuración en el servidor
SERVER	Alto	Suplantación de Certificado Digital	Interceptación de tráfico por suplantación de Certificado	Certificado SSL invalido
Cuentas del Dominio de la organización	Alto	Uso de password débiles	Acceso No Autorizado por Contraseñas débiles	Contraseñas débiles
PC'S	Bajo	Uso de herramientas de Hacking	Volcado de contenido de memoria RAM (local y remoto) y Obtención de credenciales almacenadas en procesos a partir del Volcado.	Estaciones de trabajo sin Fixes de Seguridad
Server	Alto	Uso de herramientas de Hacking	Volcado de contenido de memoria RAM (local y remoto) y Obtención de credenciales almacenadas en procesos a partir del Volcado.	Servidor sin Fixes de Seguridad
Server	Alto	Uso de herramientas de Hacking	Volcado de contenido de memoria RAM (local y remoto) y Obtención de credenciales almacenadas en procesos a partir del Volcado.	Servidor sin Fixes de Seguridad
PC	Medio	Mala Configuración de Software	Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”	Mala configuración en el servidor
PC	Medio	Mala Configuración de Software	Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”	Mala configuración en el servidor
PC'S	Medio	Mala Configuración de Software	Escalada de Privilegios mediante cuentas Administradoras Locales "XXXXX" "XXXXX" "XXX" "XXXXX" "XXXX"	Mala configuración en el servidor
PC'S	Medio	Mala Configuración de Software	Escalada de Privilegios mediante cuenta Administradora de Dominio Usuario: "XXXX", "XXXXX",	Mala configuración en el servidor

			"inv"	
Server	Alto	Vulneración de Software obsoleto	Múltiples vulnerabilidades en IBM WebSphere Application Server 6.1	Servidor Fuera de Soporte
Server	Medio	Interceptación de tráfico	Interceptación de tráfico a través de Microsoft Windows RDP Man in The Middle Vulnerability	Servidor sin Fixes de Seguridad

Tabla 14. (Continuación)

Activo de información	Impacto	Amenaza	Amenaza proveedor	Vulnerabilidades
Desktop's	Medio	Usuarios sin Password	Acceso no autorizado al sistema por usuario administrador local sin contraseña	Usuarios sin Passwords
Server	Bajo	Uso de Password de Industria	Credenciales por defecto o fáciles de averiguar "Quest Software"	Contraseñas por defecto
Server	Medio	Explotación de vulnerabilidades de software	Control sobre el sistema operativo desde la base de datos	Servidor sin Fixes de seguridad
Server	Medio	Información en texto claro	Transmisión de información sin cifrar	Falta de mecanismos de cifrado
Server	Alto	Explotación de vulnerabilidades de software	Múltiples vulnerabilidades en Oracle Database Server	Servidor sin Fixes de seguridad

Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León

7.1.3.3 Determinación de la probabilidad de ocurrencia. Para el desarrollo de este capítulo se analizaron los tipos de Incidentes de Seguridad de la información de la entidad bancaria con el fin de determinar si estos contemplan las amenazas identificadas en las pruebas de intrusión, lo anterior con el fin de calcular la probabilidad de ocurrencia basándose en datos reales respecto a la materialización de las amenazas en el ambiente tecnológico de la entidad; a continuación en la tabla 15 se muestran los tipos de incidentes de seguridad de la información definidos por la entidad bancaria que tienen relevancia respecto a las amenazas identificadas en las prueba de intrusión:

Tabla 15. Incidentes de Seguridad de la Información de la entidad bancaria

Categoría del incidente de seguridad	Descripción	Sub categoría de incidente	Detalle
Mal uso de los recursos tecnológicos del banco.	Los incidentes correspondientes a esta categoría hacen referencia al uso inadecuado de los recursos tecnológicos dispuestos por el banco para la ejecución de actividades propias del ambiente laboral.	Instalación de software no autorizado	Instalación de software específico para la omisión y/o vulneración de los controles de seguridad y componentes de la infraestructura tecnológica del banco.

Código malicioso	Los incidentes correspondientes a esta categoría hacen referencia la ejecución de software malicioso o "malware" sobre los activos de información del banco.	Malware genérico	Esta sub categoría aplica para todo tipo de código malicioso que altere el normal funcionamiento de un sistema, esta categoría debe ser aplicada siempre que el comportamiento del malware no corresponda a ninguna de las topologías detalladas en las sub categorías de código malicioso, un ejemplo es un virus genérico.

Tabla 15. (Continuación)

Categoría del incidente de seguridad	Descripción	Sub categoría de incidente	Detalle
Recolección de información	Los incidentes correspondientes a esta categoría hacen referencia a obtener información de la infraestructura tecnológica del banco; las sub categorías definidas para este tipo de incidente corresponden a situaciones de origen interno.	Sniffing interno	Observación y captura de tráfico de red.

Acceso no autorizado	Los incidentes correspondientes a esta categoría hacen referencia al compromiso, acceso y uso no autorizado de un componente de infraestructura tecnológica del banco, así como el acceso, modificación y borrado no autorizado de la información contenida en él.	Compromiso de credenciales de autenticación.	Acceso exitoso a un sistema u aplicación a través de técnicas de fuerza bruta, cracking passwords, usuarios sin contraseña, contraseñas por defecto, divulgación de credenciales de autenticación, captura de contraseñas que viajan en claro.
		Explotación de vulnerabilidades conocidas	Explotación de vulnerabilidades CVE.
		Explotación de vulnerabilidades 0 day	Explotación de nuevas vulnerabilidades 0-day, identificación de tráfico anormal.

Tabla 15. (Continuación)

Categoría del incidente de seguridad	Descripción	Sub categoría de incidente	Detalle

Acceso no autorizado	Los incidentes correspondientes a esta categoría hacen referencia al compromiso, acceso y uso no autorizado de un componente de infraestructura tecnológica del banco, así como el acceso, modificación y borrado no autorizado de la información contenida en él.	Explotación de vulnerabilidades de una aplicación.	Explotación de debilidades de seguridad en el código de las aplicaciones desarrolladas por terceros o por el banco que permitan la ejecución de xxs, inyección de código, alteración de objetos, divulgación de información, y acceso no autorizado al sistema anfitrión.
		Parámetros de configuración de los componentes de infraestructura tecnológica.	Explotación de las debilidades de seguridad originadas por la mala configuración de los parámetros de seguridad de los componentes de infraestructura tocológica del banco.
Negación de servicio	Los incidentes correspondientes a esta categoría hacen referencia a situaciones en las cuales un sistema, un servicio o una red deja de operar correctamente, causando indisponibilidad total del recurso o sistema.	Denegación de servicio (DoS)	DoS es un ataque a un sistema o red que causa que un servicio o recurso sea totalmente inaccesible a los usuarios legítimos. Esta sub categoría aplica para los ataques realizados por única fuente identificada.
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León			

En la tabla 16 se presenta la relación que existe entre los tipos de amenazas identificados en el ...Capitulo 7.1.2 ... versus los tipos de incidentes de seguridad de la información identificados en el párrafo anterior:

Tabla 16. Amenazas Versus Tipos de incidentes de seguridad de la información

Tipo de amenaza	Amenaza	Categoría del incidente de seguridad de la información	Sub categoría de incidente de seguridad
Compromiso de	Malware	Código Malicioso	Malware

componentes de TI	Explotación de vulnerabilidades de software	Acceso no autorizado	Explotación de vulnerabilidades conocidas
Software obsoleto	Vulneración de software obsoleto	Acceso no autorizado	Explotación de vulnerabilidades conocidas Explotación de vulnerabilidades 0 day
Acceso no autorizado al componente de ti	Usuarios sin Password	Acceso no autorizado	Compromiso de credenciales de autenticación.
	Uso de password débiles	Acceso no autorizado	Compromiso de credenciales de autenticación.
	Mala configuración de software	Acceso no autorizado	Parámetros de configuración de los componentes de infraestructura tecnológica.
	Uso de password de Industria	Acceso no autorizado	Compromiso de credenciales de autenticación.
Compromiso de información	Información en texto claro	N/A	N/A
	Interceptación de tráfico	Recolección de información	Sniffing Interno
	Suplantación de certificado digital	N/A	N/A
	Uso de password de industria	Acceso no autorizado	Compromiso de credenciales de autenticación.
	Uso de herramientas de Hacking	Mal uso de los recursos tecnológicos del banco.	Instalación de Software No Autorizado
Denegación de servicio	Explotación de vulnerabilidades de software	Negación de servicio	Denegación de servicio (DoS) Explotación de vulnerabilidades conocidas Explotación de vulnerabilidades 0 day
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León			

Como se puede observar en la tabla 16 solo dos tipos de amenazas: Información en texto claro y suplantación de certificado digital no coinciden de manera directa con las categorías de los incidentes de seguridad definidos en el Banco, estos dos tipos de amenazas representan el 4.87% del total de vulnerabilidades lo cual equivale a 2 vulnerabilidades de las 41 vulnerabilidades reportadas en el informe; a continuación en la tabla 17 se presentan las dos vulnerabilidades que no tienen relación directa con los incidentes de seguridad definidos en el Banco:

Tabla 17. Amenazas no contempladas en los tipos de incidentes de seguridad de la información

Activo de información	Criticidad dada por proveedor	Categoría amenaza	Tipo de amenaza	Vulnerabilidad	Vulnerabilidades
Server	Alta	Compromiso de información	Información en texto claro	Transmisión de información sin cifrar	Falta de mecanismos de cifrado
SERVER	Media	Compromiso de información	Suplantación de certificado digital	Interceptación de tráfico por suplantación de certificado	Certificado SSL invalido

Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León

Ya que el 95.13% de las vulnerabilidades reportadas tienen relación directa con los tipos de incidentes de seguridad de la información, se consideró acertado definir la probabilidad de ocurrencia con base en los incidentes de seguridad materializados en los años anteriores en la entidad; así mismo se definió que las dos vulnerabilidades que no tienen relación con los incidentes de seguridad del Banco serán tratadas con probabilidad de ocurrencia baja ya que el proceso de gestión de incidentes de seguridad no ha considerado incluir este subtipo de incidentes en el proceso por su baja probabilidad de ocurrencia.

A continuación en la tabla 18 se presenta la cantidad de incidentes de seguridad de la información que tienen relación con las amenazas identificadas en la prueba de intrusión y que fueron materializados en los últimos 5 años en el Banco:

Tabla 18. Número de incidentes de seguridad de la información

Subcategoría de incidente de seguridad	Número de incidentes
Compromiso de credenciales de autenticación.	9

Denegación de servicio (DoS)	1
Explotación de vulnerabilidades 0 day	5
Explotación de vulnerabilidades conocidas	5
Explotación de vulnerabilidades de una aplicación.	6
Instalación de software no autorizado	8
Malware genérico	30
Parámetros de configuración de los componentes de infraestructura tecnológica.	5
Sniffing Interno	1
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Como se puede observar en la tabla 18 el incidente de seguridad de la información que más se ha presentado en el Banco es el relacionado con el Malware; los menos frecuentes son la denegación de servicio y el sniffing.

Para poder definir la frecuencia con la que se presenta la materialización de cada amenaza en el Banco, fue necesario precisar la fecha en el cual se presentó cada tipo de incidente, este detalle es presentado en las tablas 19 a la 27:

Tabla 19. Fechas de ocurrencia de incidentes de tipo compromiso de credenciales de autenticación

Compromiso de credenciales de autenticación	
Fecha del Incidente	Número de Incidentes
sep-11	1
abr-12	2
jun-12	2
jun-14	4
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Tabla 20. Fecha de ocurrencia de incidentes de tipo denegación de servicio (DoS)

Denegación de servicio (DoS)	
Fecha del Incidente	Número de Incidentes
jul-14	1
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Tabla 21. Fecha de ocurrencia de incidentes de tipo explotación de vulnerabilidades 0 day

Explotación de vulnerabilidades 0 day	
Fecha del Incidente	Número de Incidentes
ago-12	1
may-14	1
nov-14	1
abr-15	1
feb-16	1
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Tabla 22. Fecha de ocurrencia de incidentes de tipo explotación de vulnerabilidades conocidas

Explotación de vulnerabilidades conocidas	
Fecha del Incidente	Número de Incidentes
ago-13	1
dic-14	1
abr-15	1
nov-15	2
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Tabla 23. Fecha de ocurrencia de incidentes de tipo explotación de vulnerabilidades de una aplicación

Explotación de vulnerabilidades de una aplicación	
Fecha del Incidente	Número de Incidentes
jul-13	2

ene-15	2
jul-15	1
ago-16	1
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Tabla 24. Fecha de ocurrencia de incidentes de tipo instalación de software no autorizado

Instalación de software no autorizado	
Fecha del Incidente	Número de Incidentes
abr-11	1
dic-11	1
abr-13	1
feb-15	1
abr-15	1
mar-16	1
sep-16	1
nov-16	1
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Tabla 25. Fecha de ocurrencia de incidentes de tipo malware genérico

Malware genérico	
Fecha del Incidente	Número de Incidentes
jul-11	3
may-12	2
jun-12	2
nov-12	1
jun-13	5
may-14	1

Tabla 25. (Continuación)

Malware genérico	
Fecha del Incidente	Número de Incidentes
may-15	3
jun-15	1

dic-15	2
ene-16	2
may-16	3
jun-16	2
jul-16	3
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Tabla 26. Fecha de ocurrencia de incidentes de tipo parámetros de configuración de los componentes de infraestructura tecnológica

Parámetros de configuración de los componentes de infraestructura tecnológica.	
Fecha del Incidente	Número de Incidentes
may-12	1
ene-13	1
mar-15	1
may-15	1
oct-16	1
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Tabla 27. Fecha de ocurrencia de incidentes de tipo sniffing interno

Sniffing interno	
Fecha del Incidente	Número de Incidentes
abr-12	1
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Con el detalle presentado de la tabla 19 a la tabla 27 referente al número de incidentes ocurridos en la entidad durante los últimos 5 años, es posible determinar el número máximo de incidentes que ocurren en el periodo de tiempo de un año para cada tipo de incidente de seguridad de la información, a continuación en la tabla 28 se presenta el número máximo de incidentes registrados en un año para cada tipo de incidente:

Tabla 28. Número máximo de incidentes registrados en un año para cada tipo de incidente de seguridad de la información

Incidente de seguridad	Máximo número de Incidentes registrado en un año
Malware genérico	10
Compromiso de credenciales de autenticación.	4
Instalación de software no autorizado	3
Explotación de vulnerabilidades de una aplicación.	2
Explotación de vulnerabilidades 0 day	2
Explotación de vulnerabilidades conocidas	2
Parámetros de configuración de los componentes de infraestructura tecnológica.	2
Denegación de servicio (DoS)	1
Sniffing Interno	1

Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León

La tabla 28 muestra la frecuencia máxima con la cual ha ocurrido cada tipo de incidente en un periodo de un año, esta relación cantidad de incidentes materializados versus tiempo transcurrido permitió establecer los criterios para la estimación de la probabilidad de ocurrencia de las amenazas, a continuación en la tabla 29 se presenta la definición cualitativa de la probabilidad de ocurrencia en razón del número máximo de incidentes materializados en un rango de tiempo medido en años:

Tabla 29. Valores cualitativos de la probabilidad de ocurrencia

Probabilidad de ocurrencia	Descripción
Bajo	Cuando ha ocurrido por lo menos una vez cada 5 años.
Madia	Cuando ha ocurrido entre 2 y 4 veces en el año.

Alta	Cuando ha ocurrido más de 4 veces en año.
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Aplicando los criterios definidos en la tabla 29 a cada tipo de incidente de seguridad identificado, se obtuvo la probabilidad de ocurrencia correspondiente como se muestra en la tabla 30:

Tabla 30. Probabilidad de ocurrencia de cata tipo de incidente de seguridad

Incidente de seguridad	Probabilidad de ocurrencia
Malware genérico	Alta
Compromiso de credenciales de autenticación.	Media
Instalación de software no autorizado	Media
Explotación de vulnerabilidades de una aplicación.	Media
Explotación de vulnerabilidades 0 day	Media
Explotación de vulnerabilidades conocidas	Media
Parámetros de configuración de los componentes de infraestructura tecnológica.	Media
Denegación de servicio (DoS)	Baja
Sniffing Interno	Baja
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

Usando la relación definida entre los tipos de amenazas y los tipos de incidentes de seguridad de la información descritos en el… Capítulo 7.1.3.3… se realizó la asignación de la probabilidad de ocurrencia a cada vulnerabilidad reportada en la prueba de instrucción como se muestra en la tabla 31:

Tabla 31. Probabilidad de ocurrencia de cada vulnerabilidad

Activo de información	Amenaza proveedor	Vulnerabilidades	Incidente de seguridad	Probabilidad de ocurrencia
server	Infección de servidor	Antivirus Inexistente o mal configurado	Malware genérico	Alta
server	Vulnerabilidad volcado de contenido de memoria RAM- obtención Tickets de Kerberos Validos	Servidor sin Fixes de seguridad	Instalación de software no autorizado Explotación de vulnerabilidades conocidas	Media
server	Volcado de memoria RAM a través de Programas ejecutados a través de RDP-compartir recursos locales.	Estaciones de trabajo mal configuradas.	Instalación de software no autorizado Explotación de vulnerabilidades conocidas	Media
server	Versión de Oracle Database obsoleta	Servidor fuera de soporte	Explotación de vulnerabilidades conocidas Explotación de vulnerabilidades 0 day	Media
PC'S	Acceso BIOS sin contraseña	Falta de autenticación en la BIOS	Compromiso de credenciales de autenticación.	Media
PC'S	Arranque de equipo de escritorio con otro sistema operativo	Falta de autenticación en la BIOS	Instalación de software no autorizado	Media
server	Versión de Microsoft Windows Server 2003 obsoleta	Servidor fuera de soporte	Explotación de vulnerabilidades conocidas explotación de vulnerabilidades 0 day	Media
server	Sesiones CIFS NULL permitidas	Mala configuración en el servidor	Compromiso de credenciales de autenticación.	Media
server	Sesiones CIFS NULL permitidas	Mala configuración en el servidor	Compromiso de credenciales de autenticación.	Media
server	Sesiones CIFS NULL permitidas	Mala configuración en el servidor	Compromiso de credenciales de autenticación.	Media
server	Sesiones CIFS NULL permitidas	Mala configuración en el servidor	Compromiso de credenciales de autenticación.	Media
server	Sesiones CIFS NULL permitidas	Mala configuración en el servidor	Compromiso de credenciales de autenticación.	Media
server	Sesiones CIFS NULL permitidas	Mala configuración en el servidor	Compromiso de credenciales de autenticación.	Media

Tabla 31. (Continuación)

Activo de información	Amenaza proveedor	Vulnerabilidades	Incidente de seguridad	Probabilidad de ocurrencia
server	Acceso no autorizado explotando vulnerabilidades del servicio VNC remoto control.	Software no autorizado instalado en el servidor	Malware/Explotación de vulnerabilidades conocidas	Alta

server	Denegación de servicio por vulnerabilidad: Apache HTTPD: Range header remoto DoS.	Servidor sin Fixes de seguridad	Explotación de vulnerabilidades conocidas/Denegación de servicio (DoS)	Media
server	Denegación de servicio por vulnerabilidad: Apache HTTPD: Range header remoto DoS.	Servidor sin Fixes de seguridad	Explotación de vulnerabilidades conocidas/Denegación de servicio (DoS)	Media
server	Suplantación de cuentas de usuario a través de SMB.	SMB signing deshabilitado	Sniffing interno	Baja
server	Suplantación de cuentas de usuario a través de SMB.	SMB signing deshabilitado	Sniffing interno	Baja
Server	Suplantación de cuentas de usuario a través de SMB.	SMB signing deshabilitado	Sniffing interno	Baja
server	Suplantación de cuentas de usuario a través de SMB.	SMB signing deshabilitado	Sniffing interno	Baja
Server	Interceptación de tráfico por vulnerabilidad Open SSL SSL/TLS MITM	Servidor sin Fixes de seguridad	Sniffing interno	Baja
Server	Servidor TLS/SSL soporta SSLv2 y SSLv3	Mala configuración en los servidores	Parámetros de configuración de los componentes de infraestructura tecnológica.	Media
Server	Interceptación de tráfico por suplantación de certificado	Certificado SSL invalido	Sniffing interno	Baja

Tabla 31. (Continuación)

Activo de información	Amenaza preveedor	Vulnerabilidades	Incidente de sseguridad	Probabilidad de ocorrencia
Server	Interceptación de tráfico por algoritmos Cipher débiles servidor TLS/SSL	Mala configuración en los servidores	Parámetros de configuración de los componentes de infraestructura	Media

			tecnológica. Sniffing interno	
Server	Interceptación de tráfico por cifrado RC4 en protocolo SSL	Mala configuración en los servidores	Parámetros de configuración de los componentes de infraestructura tecnológica. Sniffing interno	Media
SERVER	Interceptación de tráfico por suplantación de certificado	Certificado SSL invalido	Parámetros de configuración de los componentes de infraestructura tecnológica.	Media
PC'S	1) Volcado de contenido de memoria RAM (local y remoto) 2) Obtención de credenciales almacenadas en procesos	Estaciones de trabajo sin Fixes de seguridad	Instalación de software No autorizado/explotación de vulnerabilidades conocidas	Media
Server	1) Volcado de contenido de memoria RAM (local y remoto) 2) Obtención de credenciales almacenadas en procesos	Servidor sin Fixes de seguridad	Instalación de software No autorizado/Explotación de vulnerabilidades conocidas	Media
Server	1) Volcado de contenido de memoria RAM (local y remoto) 2) Obtención de credenciales almacenadas en procesos	Servidor sin Fixes de seguridad	Instalación de software No Autorizado/Explotación de vulnerabilidades conocidas	Media

Tabla 31. (Continuación)

Activo de información	Amenaza proveedor	Vulnerabilidades	Incidente de seguridad	Probabilidad de ocurrencia
PC	Escalada de privilegios en sistema operativo de equipo de escritorio	Mala configuración en los PC	Parámetros de configuración de los componentes de	Media

	mediante “Teclas especiales”		infraestructura tecnológica.	
PC	Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”	Mala configuración en los PC	Parámetros de configuración de los componentes de infraestructura tecnológica.	Media
PC'S	Escalada de privilegios mediante cuentas Administradoras Locales "XXXXX" "XXXXX" "XXX" "XXXXX" "XXXX"	Mala configuración en los PC	Parámetros de configuración de los componentes de infraestructura tecnológica/Explotación de vulnerabilidades conocidas	Media
Server	Interceptación de tráfico a través de Microsoft Windows RDP Man in The Middle	Servidor sin Fixes de seguridad	Sniffing Interno	Baja
Server	Interceptación de tráfico a través de Microsoft Windows RDP Man in The Middle Vulnerability	Servidor sin Fixes de seguridad	Sniffing Interno	Baja
Desktop's	Acceso no autorizado al sistema por usuario administrador local sin contraseña	Usuarios sin Passwords	Compromiso de credenciales de autenticación.	Media
Server	Credenciales por defecto o fáciles de averiguar "Quest Software"	Contraseñas por defecto	Compromiso de credenciales de autenticación.	Media
Server	Control sobre el sistema operativo desde la base de datos	Servidor sin Fixes de seguridad	Explotación de vulnerabilidades conocidas	Media

Tabla 31. (Continuación)

Activo de información	Amenaza proveedor	Vulnerabilidades	Incidente de seguridad	Probabilidad de ocurrencia
PC'S	Escalada de privilegios mediante cuenta administradora de	Mala configuración en los PC	Parámetros de configuración de los componentes de	Media

	dominio usuario: "XXXX", "XXXXX", "inv"		infraestructura tecnológica/Explotación de vulnerabilidades conocidas	
Server	Múltiples vulnerabilidades en IBM WebSphere Application Server 6.1	Servidor fuera de soporte	Explotación de vulnerabilidades conocidas Explotación de vulnerabilidades 0 day	Media
Server	Transmisión de información sin cifrar	Falta de mecanismos de cifrado	Sniffing Interno	Baja
Server	Múltiples vulnerabilidades en Oracle Database Server	Servidor sin Fixes de seguridad	Explotación de vulnerabilidades conocidas	Media
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

7.1.3.4 Determinación del riesgo. Para la estimación del riesgo se utilizó la definición establecida en el ... Capítulo 6.3.5… la cual indica que se requieren dos variables: el impacto, que fue determinado en el … Capitulo 7.1.3.2… y la probabilidad de ocurrencia que fue determinada en el … Capitulo 7.1.3.3…; en el … Anexo B… se detalla la matriz de determinación del riesgo para cada vulnerabilidad.

A continuación en la tabla 32 se presenta el resultado del riesgo de cada vulnerabilidad:

Tabla 32. Nivel de riesgo por vulnerabilidad

IP	Activo de información	Amenaza	Amenaza proveedor	Vulnerabilidades	Riesgo
x.x.x.x	server	Malware	Infección de servidor	Antivirus inexistente o mal configurado	Alto
x.x.x.x	server	Uso de herramientas de Hacking	Volcado de contenido de memoria RAM-obtención Tickets de Kerberos Validos	Servidor sin Fixes de seguridad	Alto
x.x.x.x	server	Uso de herramientas de Hacking	Volcado de memoria RAM a través de Programas ejecutados a través de RDP-compartir recursos locales.	Estaciones de trabajo mal configuradas.	Alto
x.x.x.x	server	Vulneración de software obsoleto	Versión de Oracle Database Obsoleta	Servidor fuera de soporte	Alto
550 Activos	PC'S	Usuarios sin Password	Acceso BIOS sin contraseña	Falta de autenticación en la BIOS	Medio
550 Activos	PC'S	Uso de herramientas de Hacking	Arranque de equipo de escritorio con otro Sistema operativo	Falta de autenticación en la BIOS	Medio
x.x.x.x	server	Vulneración de software obsoleto	Versión de Microsoft Windows Server 2003 obsoleta	Servidor Fuera de Soporte	Alto
x.x.x.x	server	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el Servidor	Medio
x.x.x.x	server	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el Servidor	Medio
x.x.x.x	server	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el Servidor	Alto
x.x.x.x	server	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el Servidor	Alto
x.x.x.x	server	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el Servidor	Alto
x.x.x.x	server	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el Servidor	Alto

Tabla 32. (Continuación)

IP	Activo de Información	Amenaza	Amenaza Proveedor	Vulnerabilidades	Riesgo
x.x.x.x	server	Explotación de vulnerabilidades de software	Acceso no autorizado explotando vulnerabilidades del servicio VNC remote control.	Software no autorizado instalado en el servidor	Alto
x.x.x.x	server	Explotación de vulnerabilidades de software	Denegación de servicio por vulnerabilidad: Apache HTTPD: Range header remote DoS.	Servidor sin Fixes de Seguridad	Alto
x.x.x.x	server	Explotación de vulnerabilidades de software	Denegación de servicio por vulnerabilidad: Apache HTTPD: Range header remote DoS.	Servidor sin Fixes de Seguridad	Medio
x.x.x.x	server	Interceptación de trafico	Suplantación de cuentas de usuario a través de SMB.	SMB signing deshabilitado	Bajo
x.x.x.x	server	Interceptación de trafico	Suplantación de cuentas de usuario a través de SMB.	SMB signing deshabilitado	Medio
x.x.x.x	Server	Interceptación de trafico	Suplantación de cuentas de usuario a través de SMB.	SMB signing deshabilitado	Bajo
x.x.x.x	server	Interceptación de trafico	Suplantación de cuentas de usuario a través de SMB.	SMB signing deshabilitado	Bajo
x.x.x.x	Server	Interceptación de trafico	Interceptación de tráfico por vulnerabilidad OpenSSL SSL/TLS MITM	Servidor sin Fixes de Seguridad	Bajo
x.x.x.x	Server	Interceptación de trafico	Servidor TLS/SSL soporta SSLv2 y SSLv3	Mala configuración en los servidores	Medio
x.x.x.x	Server	Interceptación de trafico	Interceptación de tráfico por suplantación de certificado	Certificado SSL invalido	Alto
x.x.x.x	Server	Interceptación de trafico	Interceptación de tráfico por algoritmos Cipher débiles servidor TLS/SSL	Mala configuración en los servidores	Medio

Tabla 32. (Continuación)

IP	Activo de Información	Amenaza	Amenaza Proveedor	Vulnerabilidades	Riesgo
x.x.x.x	Server	Interceptación de trafico	Interceptación de tráfico por cifrado RC4 en protocolo SSL	Mala configuración en los servidores	Medio
x.x.x.x:8443	SERVER	Suplantación de certificado digital	Interceptación de tráfico por suplantación de certificado	Certificado SSL invalido	Medio
Cuentas del Dominio de la organización	Cuentas del Dominio de la organización	Uso de password débiles	Acceso no autorizado por contraseñas débiles	Contraseñas débiles	Alto
550 Activos	PC'S	Uso de herramientas de Hacking	Volcado de contenido de memoria RAM (local y remoto) y obtención de credenciales almacenadas en procesos a partir del volcado.	Estaciones de trabajo sin Fixes de seguridad	Bajo
x.x.x.x	Server	Uso de herramientas de Hacking	Volcado de contenido de memoria RAM (local y remoto) y obtención de credenciales almacenadas en procesos a partir del volcado.	Servidor sin Fixes de Seguridad	Alto
x.x.x.x	Server	Uso de herramientas de Hacking	Volcado de contenido de memoria RAM (local y remoto) y obtención de credenciales almacenadas en procesos a partir del volcado.	Servidor sin Fixes de Seguridad	Alto
x.x.x.x	PC	Mala configuración de software	Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”	Mala configuración en los PC	Medio
x.x.x.x	PC	Mala configuración de software	Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”	Mala configuración en los PC	Medio

Tabla 32. (Continuación)

IP	Activo de Información	Amenaza	Amenaza Proveedor	Vulnerabilidades	Riesgo
550 Activos	PC'S	Mala configuración de software	Escalada de Privilegios mediante cuentas administradoras locales "XXXXX" "XXXXX" "XXXX" "XXXXX""XXXX"	Mala configuración en los PC	Medio
550 Activos	PC'S	Mala configuración de software	Escalada de Privilegios mediante cuenta administradora de dominio Usuario: "XXXX", "XXXXX", "inv"	Mala configuración en los PC	Medio
x.x.x.x	Server	Vulneración de software obsoleto	Múltiples vulnerabilidades en IBM WebSphere Application Server 6.1	Servidor Fuera de Soporte	Alto
x.x.x.x	Server	Interceptación de trafico	Interceptación de tráfico a través de Microsoft Windows RDP Man in The Middle	Servidor sin Fixes de Seguridad	Bajo
x.x.x.x	Server	Interceptación de trafico	Interceptación de tráfico a través de Microsoft Windows RDP Man in The Middle Vulnerability	Servidor sin Fixes de Seguridad	Bajo
500 Activos	Desktop's	Usuarios sin Password	Acceso no Autorizado al sistema por usuario administrador local sin contraseña	Usuarios sin Passwords	Medio
x.x.x.x	Server	Uso de password de industria	Credenciales por defecto o fáciles de averiguar "Quest Software"	Contraseñas por defecto	Bajo

Tabla 32. (Continuación)

IP	Activo de Información	Amenaza	Amenaza Proveedor	Vulnerabilidades	Riesgo
x.x.x.x	Server	Explotación de vulnerabilidades de software	Control sobre el sistema operativo desde la base de datos	Servidor sin Fixes de Seguridad	Medio
x.x.x.x	Server	Información en texto claro	Transmisión de información sin cifrar	Falta de mecanismos de cifrado	Bajo
x.x.x.x	Server	Explotación de vulnerabilidades de software	Múltiples vulnerabilidades en Oracle Database server	Servidor sin Fixes de Seguridad	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

7.1.3.5 Vulnerabilidades críticas. De acuerdo al de riesgo calculado en el... Capítulo 7.1.3.4... fue posible determinar las vulnerabilidades críticas a trabajar en los siguientes capítulos, a continuación en la tabla 33 se presentan las vulnerabilidades en las cuales el riesgo fue alto:

Tabla 33. Vulnerabilidades Críticas

IP	Activo de información	Amenaza	Amenaza proveedor	Vulnerabilidades	Riesgo
x.x.x.x	server	Malware	Infección de servidor	Antivirus Inexistente o mal configurado	Alto
x.x.x.x	server	Uso de herramientas de Hacking	Volcado de contenido de memoria RAM	Servidor sin Fixes de seguridad	Alto
x.x.x.x	server	Uso de herramientas de Hacking	Volcado de memoria RAM a través de programas ejecutados a través de RDP-compartir recursos locales.	Estaciones de trabajo Mal configuradas.	Alto

Tabla 33. (Continuación)

IP	Activo de información	Amenaza	Amenaza proveedor	Vulnerabilidades	Riesgo
x.x.x.x	server	Vulneración de software obsoleto	Versión de Oracle Database obsoleta	Servidor fuera de soporte	Alto
x.x.x.x	server	Vulneración de software obsoleto	Versión de Microsoft Windows Server 2003 obsoleta	Servidor fuera de soporte	Alto
x.x.x.x	server	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el servidor	Alto
x.x.x.x	server	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el servidor	Alto
x.x.x.x	server	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el servidor	Alto
x.x.x.x	Server	Uso de password de industria	Sesiones CIFS NULL permitidas	Mala configuración en el servidor	Alto
x.x.x.x	server	Explotación de vulnerabilidades de software	Acceso no autorizado explotando vulnerabilidades del Servicio VNC remote control.	Software no autorizado instalado en el servidor	Alto
x.x.x.x	server	Explotación de vulnerabilidades de Software	Denegación de servicio por vulnerabilidad: Apache HTTPD: Range header remote DoS.	Servidor sin Fixes de seguridad	Alto
x.x.x.x	Server	Interceptación de tráfico	Interceptación de tráfico por suplantación de certificado	Certificado SSL invalido	Alto
Cuentas del Dominio de la organización	Cuentas del Dominio de la organización	Uso de password débiles	Acceso no autorizado por contraseñas débiles	Contraseñas débiles	Alto
x.x.x.x	Server	Uso de herramientas de Hacking	Volcado de contenido de memoria RAM (local y remoto) y obtención de credenciales almacenadas en procesos a partir del Volcado.	Servidor sin Fixes de seguridad	Alto

Tabla 33. (Continuación)

IP	Activo de información	Amenaza	Amenaza proveedor	Vulnerabilidades	Riesgo
x.x.x.x	Server	Uso de herramientas de Hacking	Volcado de contenido de memoria RAM (local y remoto) y Obtención de credenciales almacenadas en procesos a partir del Volcado.	Servidor sin Fixes de seguridad	Alto
x.x.x.x	Server	Vulneración de software obsoleto	Múltiples vulnerabilidades en IBM WebSphere Application Server 6.1	Servidor Fuera de soporte	Alto
x.x.x.x	Server	Explotación de vulnerabilidades de software	Múltiples vulnerabilidades en Oracle Database Server	Servidor sin Fixes de seguridad	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

7.2 ESTABLECIMIENTO DE LOS CONTROLES A IMPLEMENTAR

En esta parte del capítulo se presenta la identificación de controles y la evaluación del riesgo residual para cada una de las vulnerabilidades criticas identificadas en el…Capítulo 7.1.3.5...

Para la definición del control a implementar se definieron las siguientes 3 actividades:

- Identificación del control recomendado por el consultor.
- Evaluar la viabilidad técnica de implantación con la Gerencia de Infraestructura, Gerencia de Telemática y Gerencia de Desarrollo Según corresponda.
- Evaluar el riesgo residual y aceptación del riesgo.

En el … Anexo C… se presentan los controles recomendados por el proveedor, así como el estudio de la viabilidad técnica de implementación realizado; en la tabla 34 se presenta el cálculo del riesgo residual de acuerdo a las definiciones

establecidas en el…Capítulo 6.5.6.1…Gestión del Riesgo - Cálculo Riesgo Residual para todas las vulnerabilidades críticas:

Tabla 34. Controles y riesgo residual

Servidor	Amenaza	Criticidad amenaza	Controles implementados	Efectividad del control	Promedio efectividad controles	Riesgo residual
server	Infección de servidor	3	Antivirus en los servidores (Control Vulnerado)	0	2	1
			Filtro de archivos ejecutables entrantes por correo electrónico.	3		
			Bloqueo de descarga de archivos en la navegación WEB para servidores.	3		
			Bloqueo de aplicaciones y archivos ejecutables a través del Symantec End Point (Control a implementar)	2		
server	Volcado de contenido de memoria RAM-obtención Tickets de Kerberos validos	3	Configuración de los Tickets de Kerberos con los siguientes parámetros: Maximum Lifetime for Service Ticket: 10 horas Maximum Lifetime: 7 días Maximum Tolerance for Computer Clock Synchronization: 5 min. Maximum lifetime for user ticket renewal 7 days	3	2,5	0,5
			Bloqueo de aplicaciones y archivos ejecutables a través del Symantec End Point (Control a implementar)	2		

Tabla 34. (Continuación)

Servidor	amenaza	Criticidad amenaza	Controles implementados	Efectividad del control	Promedio efectividad controles	Riesgo residual
server	Volcado de memoria RAM a través de programas ejecutados a través de RDP-compartir recursos locales	3	Aplicación de una GPO para restringir el uso de carpetas compartidas en sesiones de terminal server	3	2,5	0,5
Server	Versión de Oracle Database Obsoleta	3	Migrar el motor de Base de datos a OracleDatabase11gEnterpriseEditionRelease11.2.0.4.0-64bit	3	3	0
server	Versión de Microsoft Windows Server 2003 obsoleta	3	Actualizar el Sistema a Windows Server 2012	3	3	0
server	Sesiones CIFS NULL permitidas	3	Implementar la llave de registro: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA Value Name: RestrictAnonymous Type: DWORD Value: 0	3	3	0
server	Sesiones CIFS NULL permitidas	3	Implementar la llave de registro: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA Value Name: RestrictAnonymous Type: DWORD Value: 0	3	3	0
server	Sesiones CIFS NULL permitidas	3	Implementar la llave de registro: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA Value Name: RestrictAnonymous Type: DWORD	3	3	0

Tabla 34. (Continuación)

Servidor	Amenaza	Criticidad Amenaza	Controles Implementados	Efectividad del Control	Promedio efectividad Controles	Riesgo Residual
server	Sesiones CIFS NULL permitidas	3	Implementar la llave de registro: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA Value Name: RestrictAnonymous Type: DWORD Value: 0	3	3	0
Server	Acceso no autorizado explotando vulnerabilidades del Servicio VNC remote control.	3	El servicio VNC fue desinstalado del servidor Server en Noviembre del 2016	3	2,5	0,5
			Uso de otro programa de conexión remota más seguro como RDP.	2		
Server	Denegación de servicio por vulnerabilidad: Apache HTTPD: Range header	3	Actualizar Apache HTTPD a la última versión disponible	2	2,5	0,5
			Realizar migración del contenedor	3		
Cuentas del dominio de la organización	Acceso no autorizado por contraseñas débiles	3	Definición de Política de Seguridad de los parámetros de complejidad de las contraseñas como longitud, caracteres especiales, números, mayúsculas.	1	2,3	0,7
			Realizar un diccionario de palabras excluidas como passwords.	3		
			Implementar en la herramienta de administración de cuentas del Banco los controles definidos en la política	3		

Tabla 34. (Continuación)

Servidor	Amenaza	Criticidad Amenaza	Controles Implementados	Efectividad del Control	Promedio efectividad Controles	Riesgo Residual
Server	Interceptación de tráfico por suplantación de certificado	3	Adquirir o generar un certificado apropiado para este servicio	3	3	0
Server	Volcado de contenido de memoria RAM (local y remoto) y Obtención de credenciales almacenadas en procesos a partir del Volcado-Servidor Server	3	Aplicar el parche del fabricante 2871997 en el servidor de dominio el cual posee el S.O. Windows Server 2008 R2, para mejorar la protección y la gestión de las credenciales. https://support.microsoft.com/en-us/kb/2871997	3	2	1
			Actualizar el S.O. del servidor de dominio a la versión Windows Server 2012 R2, para utilizar el grupo de usuarios llamado: Protected User Security Group	1		
Server	Volcado de contenido de memoria RAM (local y remoto) y Obtención de credenciales almacenadas en procesos a partir del Volcado-Servidor	3	Aplicar el parche del fabricante 2871997 en el servidor de dominio el cual posee el S.O. Windows Server 2008 R2, para mejorar la protección y la gestión de las credenciales. https://support.microsoft.com/en-us/kb/2871997	3	2	1
			Actualizar el S.O. del servidor de dominio a la versión Windows Server 2012 R2, para utilizar el grupo de usuarios llamado: Protected User Security Group	1		

Tabla 34. (Continuación)

Servidor	Amenaza	Criticidad Amenaza	Controles Implementados	Efectividad del Control	Promedio efectividad Controles	Riesgo Residual
Server	Múltiples vulnerabilidades en IBM WebSphere Application Server 6.1	3	Se recomienda mantener el software actualizado, ya sea mediante parches de seguridad o instalando las versiones más recientes del producto. Si se utiliza el software WebSphere Application Server, aplicar el Fix Pack 33 (6.1.0.33) o posterior.	3	2	1
			Si se utiliza el paquete embebido de WebSphere Application Server con Tivoli Directory Server, aplicar el ultimo Fix Pack eWAS recomendado	1		
Server	Múltiples vulnerabilidades en Oracle Database Server	3	Se recomienda mantener el software actualizado, ya sea mediante parches de seguridad.	3	3	0
			Realizar la instalación de las versiones más recientes de Oracle	3		
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León						

7.3 DETERMINACIÓN DE LAS FECHAS DE REMEDIACIÓN DE LAS VULNERABILIDADES

En esta parte del capítulo se establecen las fechas en las cuales se van a remediar las vulnerabilidades.

Para establecer las fechas en las cuales se pueden implementar los controles se tuvieron en cuenta los días en los cuales el Banco tiene permitido hacer cambios de infraestructura tecnológica, festividades de fin de año y pruebas de contingencia.

A continuación se presentan los acuerdos pactados con cada una de las áreas del Banco involucradas para dar solución y/o mitigación a cada una de las vulnerabilidades críticas.

En la tabla 35 presenta la fecha establecida para la implementación de los controles definidos para cada vulnerabilidad trabajada.

Tabla 35. Fechas de implementación de los controles

Servidor	Amenaza	Criticidad amenaza	Controles implementados	Fecha de implementación
server	Infección de servidor	3	Antivirus en los servidores (Control Vulnerado)	N/A
			Filtro de archivos ejecutables entrantes por correo electrónico	31/09/2016
			Bloqueo de descarga de archivos en la navegación WEB.	31/09/2016
			Bloqueo de aplicaciones y archivos ejecutables a través del Symantec End Point (Control a implementar)	31/09/2016
server	Volcado de contenido de memoria RAM-obtención Tickets de Kerberos Validos	3	Configuración de los Tickets de Kerberos con los siguientes parámetros: Maximum Lifetime for Service Ticket: 10 horas Maximum Lifetime: 7 dias Maximum Tolerance for Computer Clock Synchronization: 5 min. Maximum lifetime for user ticket renewal 7 days	28/02/2017
			Bloqueo de aplicaciones y archivos ejecutables a través del Symantec End Point (Control a implementar)	31/09/2016

Tabla 35. (Continuación)

Servidor	Amenaza	Criticidad amenaza	Controles implementados	Fecha de implementación
server	Volcado de memoria RAM a través de programas ejecutados a través de RDP-compartir recursos locales	3	Aplicación de una GPO para restringir el uso de carpetas compartidas en sesiones de terminal server	28/02/2017
			Bloqueo de aplicaciones y archivos ejecutables a través del Symantec End Point (Control a implementar)	31/09/2016
Server	Versión de Oracle Database obsoleta	3	Migrar el motor de base de datos a OracleDatabase11gEnterpriseEditionRelease11.2.0.4.0-64bit	31/01/2017
server	Versión de Microsoft Windows Server 2003 obsoleta	3	Actualizar el sistema a Windows Server 2012	28/02/2017
server	Sesiones CIFS NULL permitidas	3	Implementar la llave de registro: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA Value Name: RestrictAnonymous Type: DWORD Value: 0	28/02/2017
server	Sesiones CIFS NULL permitidas	3	Implementar la llave de registro: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA Value Name: RestrictAnonymous Type: DWORD Value: 0	28/02/2017
server	Sesiones CIFS NULL permitidas	3	Implementar la llave de registro: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA Value Name: RestrictAnonymous Type: DWORD Value: 0	28/02/2017

Tabla 35. (Continuación)

Servidor	Amenaza	Criticidad amenaza	Controles implementados	Fecha de implementación
server	Sesiones CIFS NULL permitidas	3	Implementar la llave de registro: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA Value Name: RestrictAnonymous Type: DWORD Value: 0	28/02/2017
Server	Acceso no autorizado explotando vulnerabilidades del servicio VNC remote control.	3	El servicio VNC fue desinstalado del servidor Server en Noviembre del 2016	30/11/2016
			Uso de otro programa de conexión remota más seguro como RDP.	N/A
Server	Denegación de servicio por vulnerabilidad: Apache HTTPD: Range header remote DoS.	3	Actualizar Apache HTTPD a la última versión disponible	N/A
			Realizar migración del contenedor	28/02/2017
Server	Interceptación de tráfico por suplantación de certificado	3	Adquirir o generar un certificado apropiado para este servicio	N/A
			Migración de plataforma a otro fabricante	30/03/2017
Cuentas del dominio de la organización	Acceso no autorizado por contraseñas débiles	3	Definición de política de Seguridad de los parámetros de complejidad de las contraseñas como longitud, caracteres especiales, números, mayúsculas.	28/02/2017
			Realizar un diccionario de palabras excluidas como passwords.	30/01/2017
			Implementar en la herramienta de administración de cuentas del banco los controles definidos en la política	30/06/2017

Tabla 35. (Continuación)

Servidor	Amenaza	Criticidad Amenaza	Controles Implementados	Fecha de Implementación
Server	Volcado de contenido de memoria RAM (local y remoto) y Obtención de credenciales almacenadas en procesos a partir del volcado-servidor Server	3	Aplicar el parche del fabricante 2871997 en el servidor de dominio el cual posee el S.O. Windows Server 2008 R2, para mejorar la protección y la gestión de las credenciales. https://support.microsoft.com/en-us/kb/2871997	30/03/2017
			Actualizar el S.O. del servidor de dominio a la versión Windows Server 2012 R2, para utilizar el grupo de usuarios llamado: Protected User Security Group	N/A
Server	Volcado de contenido de memoria RAM (local y remoto) y obtención de credenciales almacenadas en procesos a partir del volcado-servidor Server	3	Aplicar el parche del fabricante 2871997 en el servidor de dominio el cual posee el S.O. Windows Server 2008 R2, para mejorar la protección y la gestión de las credenciales. https://support.microsoft.com/en-us/kb/2871997	30/03/2017
			Actualizar el S.O. del servidor de dominio a la versión Windows Server 2012 R2, para utilizar el grupo de usuarios llamado: Protected User Security Group	N/A
Server	Múltiples vulnerabilidades en IBM WebSphere Application Server 6.1	3	Se recomienda mantener el software actualizado, ya sea mediante parches de seguridad o instalando las versiones más recientes del producto. Si se utiliza el software WebSphere Application Server, aplicar el Fix Pack 33 (6.1.0.33) o posterior.	30/10/2017
			Si se utiliza el paquete embebido de WebSphere Application Server con Tivoli Directory Server, aplicar el ultimo Fix Pack eWAS recomendado	N/A
Server	Múltiples vulnerabilidades en Oracle Database Server	3	Se recomienda mantener el software actualizado, ya sea mediante parches de seguridad.	30/06/2017
			Realizar la instalación de las versiones más recientes de Oracle	N/A

Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León

7.4 ELABORACIÓN DEL PLAN DE REMEDIACIÓN

En esta parte del capítulo se presenta el plan de remediación propuesto para la remediación las vulnerabilidades críticas producto de análisis hecho en el desarrollo del presente proyecto. En la tabla 36 se evidencia en su totalidad cada una de las vulnerabilidades trabajadas con su correspondiente control para solución, fecha de mitigación y área con la cual se generó el compromiso de solución a la vulnerabilidad.

Tabla 36. Plan de remediación para las vulnerabilidades críticas

Servidor	Amenaza	Criticidad amenaza	Controles implementados	Fecha de implementación	Responsable
Server	Infección de servidor	3	Filtro de archivos ejecutables entrantes por correo electrónico	31/11/2016	Dirección de seguridad informática
			Bloqueo de descarga de archivos en la navegación WEB.	31/11/2016	Dirección de seguridad informática
			Bloqueo de aplicaciones y archivos ejecutables a través del Symantec End Point (Control a implementar)	31/11/2016	Jefatura de equipos
Server	Volcado de contenido de memoria RAM-obtención Tickets de Kerberos validos	3	Configuración de los Tickets de Kerberos con los siguientes parámetros: Maximum Lifetime for Service Ticket: 10 horas Maximum Lifetime: 7 días Maximum Tolerance for Computer Clock Synchronization: 5 min. Maximum lifetime for user ticket renewal 7 days	28/02/2017	Gerencia de infraestructura
			Bloqueo de aplicaciones y archivos ejecutables a través del Symantec End Point (Control a implementar)	31/09/2016	Jefatura de equipos

Tabla 36. (Continuación)

Servidor	Amenaza	Criticidad amenaza	Controles implementados	Fecha de implementación	Responsable
server	Volcado de memoria RAM a través de programas ejecutados a través de RDP-compartir recursos locales	3	Aplicación de una GPO para restringir el uso de carpetas compartidas en sesiones de terminal server	28/02/2017	Gerencia de Infraestructura
			Bloqueo de aplicaciones y archivos ejecutables a través del Symantec End Point (Control a implementar)	31/09/2016	Jefatura de equipos
Server	Versión de Oracle Database obsoleta	3	Migrar el motor de base de datos a OracleDatabase11gEnterpriseEditionRelease11.2.0.4.0-64bit	31/01/2017	Jefatura de Administración de Bases de datos
server	Versión de Microsoft Windows Server 2003 obsoleta	3	Actualizar el sistema a Windows Server 2012	28/02/2017	Gerencia de Infraestructura
server	Sesiones CIFS NULL permitidas	3	Implementar la llave de registro: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA Value Name: RestrictAnonymous Type: DWORD Value: 0	28/02/2017	Gerencia de Infraestructura
server	Sesiones CIFS NULL permitidas	3	Implementar la llave de registro: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA Value Name: RestrictAnonymous Type: DWORD Value: 0	28/02/2017	Gerencia de Infraestructura

Tabla 36. (Continuación)

Servidor	Amenaza	Criticidad amenaza	Controles implementados	Fecha de implementación	Responsable
server	Sesiones CIFS NULL permitidas	3	Implementar la llave de registro: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA Value Name: RestrictAnonymous Type: DWORD Value: 0	28/02/2017	Gerencia de infraestructura
server	Sesiones CIFS NULL permitidas	3	Implementar la llave de registro: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA Value Name: RestrictAnonymous Type: DWORD Value: 0	28/02/2017	Gerencia de infraestructura
Server	Acceso no autorizado explotando vulnerabilidades del servicio VNC remote control.	3	El servicio VNC fue desinstalado del servidor Server en Noviembre del 2016	30/11/2016	Gerencia de infraestructura - Administración de servidores
			Uso de otro programa de conexión remota más seguro como RDP.	N/A	
Server	Denegación de servicio por vulnerabilidad: Apache HTTPD: Range header remote DoS.	3	Actualizar Apache HTTPD a la última versión disponible	N/A	Gerencia de infraestructura - Administración de base de datos y contenedores
			Realizar migración del contenedor	28/02/2017	
Server	Interceptación de tráfico por suplantación de certificado	3	Adquirir o generar un certificado apropiado para este servicio	N/A	Dirección de seguridad informática
			Migración de plataforma a otro fabricante	30/03/2017	

Tabla 36. (Continuación)

Servidor	Amenaza	Criticidad amenaza	Controles implementados	Fecha de implementación	Responsable
Cuentas del dominio de la organización	Acceso no autorizado por contraseñas débiles	3	Definición de política de seguridad de los parámetros de complejidad de las contraseñas como longitud, caracteres especiales, números, mayúsculas.	28/02/2017	Dirección de seguridad de la información
			Realizar un diccionario de palabras excluidas como passwords.	30/01/2017	Jefatura de equipos
			Implementar en la herramienta de administración de cuentas del Banco los controles definidos en la política	30/06/2017	
Server	Volcado de contenido de memoria RAM (local y remoto) y obtención de credenciales almacenadas en procesos a partir del volcado-servidor Server	3	Aplicar el parche del fabricante 2871997 en el servidor de dominio el cual posee el S.O. Windows Server 2008 R2, para mejorar la protección y la gestión de las credenciales. https://support.microsoft.com/en-us/kb/2871997	30/03/2017	Gerencia de infraestructura-Administración de servidores
			Actualizar el S.O. del servidor de dominio a la versión Windows Server 2012 R2, para utilizar el grupo de usuarios llamado: Protected User Security Group	N/A	
Server	Volcado de contenido de memoria RAM (local y remoto) y obtención de credenciales almacenadas en procesos a partir del volcado-servidor Server	3	Aplicar el parche del fabricante 2871997 en el servidor de dominio el cual posee el S.O. Windows Server 2008 R2, para mejorar la protección y la gestión de las credenciales. https://support.microsoft.com/en-us/kb/2871997	30/03/2017	Gerencia de infraestructura-Administración de servidores
			Actualizar el S.O. del servidor de dominio a la versión Windows Server 2012 R2, para utilizar el grupo de usuarios llamado: Protected User Security Group	N/A	

Tabla 36. (Continuación)

Servidor	Amenaza	Criticidad amenaza	Controles implementados	Fecha de implementación	Responsable
Server	Múltiples vulnerabilidades en IBM WebSphere Application Server 6.1	3	Se recomienda mantener el software actualizado, ya sea mediante parches de seguridad o instalando las versiones más recientes del producto.	30/10/2017	Gerencia de infraestructura-Administración de base de datos y contenedores
			Si se utiliza el software WebSphere Application Server, aplicar el Fix Pack 33 (6.1.0.33) o posterior.		
			Si se utiliza el paquete embebido de WebSphere Application Server con Tivoli Directory Server, aplicar el ultimo Fix Pack eWAS recomendado	N/A	
Server	Múltiples vulnerabilidades en Oracle Database Server	3	Se recomienda mantener el software actualizado, ya sea mediante parches de seguridad.	30/06/2017	Gerencia de infraestructura-Administración de base de datos y contenedores
			Realizar la instalación de las versiones más recientes de Oracle	N/A	
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

8. CONCLUSIONES

- En el desarrollo del proyecto se construyó una metodología que permite tratar de manera eficiente las vulnerabilidades explotadas en la prueba de intrusión, priorizando el tratamiento de las amenazas que mayor impacto y probabilidad de ocurrencia pueden tener en el ambiente tecnológico del banco.

- La metodología propuesta para la gestión de vulnerabilidades críticas a partir del cálculo del riesgo, permitió a la entidad bancaria definir los controles que se deben implementar con el fin de garantizar la reducción del riesgo a niveles aceptables por el Banco, así como la aplicabilidad tecnológica del mismo.

- Las vulnerabilidades reportadas por el proveedor son categorizadas respecto a su severidad según el estándar CVSS v2.0, sin embargo en esta calificación no se tuvo en cuenta la criticidad de los activos del Banco, la cantidad de equipos afectados, ambiente de producción, entre otros, por lo cual se recalculo la severidad empleando las métricas base, temporal y de entorno definidas por el mismo estándar con el fin de establecer la severidad real aplicada al ambiente tecnológico de la entidad, esta actividad permitió concluir que la métrica de entorno posee mayor porcentaje de ponderación respecto a las otras métricas, razón por la cual la severidad obtenida después del proceso aplicado difiere de la severidad reportada inicialmente por el Proveedor.

- Empleando la metodología propuesta se obtuvo una diferencia del 39.2% entre las vulnerabilidades reportadas como críticas por el proveedor (28) y las vulnerabilidades consideradas críticas para la entidad (17), esto tiene una importancia significativa para la Vicepresidencia de Tecnología, ya que como se pudo observar en el …Capitulo 8.3 … algunos controles consisten en adquirir e implementar nuevas herramientas de seguridad como el filtro de contenido Web, así como la migración de algunas aplicaciones críticas para el Banco, lo cual sin este estudio no se hubiera asignado la celeridad adecuada.

- Involucrar de manera directa a los responsables de la implementación del control desde la fase de evaluación y definición del mismo, permitió generar un plan de remediación que se ajusta a la realidad del Banco y su ambiente tecnológico, generando compromiso de las partes involucradas a fin de garantizar que no se generaran mayores incumplimientos en las fechas establecidas en dicho plan.

- Gran parte de la metodología desarrollada en esta investigación fue diseñada con base en la norma ISO 27005, esta norma enmarca la gestión de riesgos de seguridad de la información para una organización ajustándose a los procesos definidos en la norma ISO 27001, sin embargo se puede concluir que es

aplicable a micro procesos que requieren una valoración del riesgo como los procesos de gestión de vulnerabilidades, gestión de pruebas de penetración y/o procesos de gestión de incidentes.

BIBLIOGRAFÍA

ALVEY, Robert. The Art of Web Filtering [en línea]. GSEC Practical v1.4b. SANS Institute InfoSec Reading Room, February 9, 2004. Disponible en Internet: URL <https://www.sans.org/reading-room/whitepapers/bestprac/art-web-filtering-1375>

ARKIN, Ofir. Evasión de controles de NAC Network Access Control. [en línea]. Insightix. 2006-2007 Disponible en Internet: URL<https://www.blackhat.com/presentations/bh-dc-07/Arkin/Presentation/bh-dc-07-Arkin-ppt-up.pdf>

CERT, Software Engineering Institute Carnegie Mellon University. Vulnerability Notes Database Field Description. [en línea]. Cert. Disponible en Internet: URL <http://www.kb.cert.org/vuls/html/fieldhelp>

COLLYER, Tim. Airwatch MDM and Android: a policy and technical review. [en línea]. GSEC. SANS Institute InfoSec Reading Room July 11. 2014. Disponible en Internet: URL <https://www.sans.org/reading-room/whitepapers/pda/airwatch-mdm-android-policy-technical-review-35372>.

CROMO. Así fracasó el robo informático al Banco de Bangladesh. [en línea]. Cromo. Abril 27, 2016. Disponible en Internet: URL<http://www.cromo.com.uy/asi-fracaso-el-robo-informatico-al-banco-bangladesh-n902149>

EL PAIS, Los piratas que robaron 73 millones al banco central de Bangladesh 'hackearon' una impresora clave. [en línea]. El País. Marzo 17, 2016. Disponible en Internet: URL<http://economia.elpais.com/economia/2016/03/17/actualidad/1458200294_374693.html>

XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016.

XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016.

XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016.

XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016

HOLLAND, Ted. Understanding IPS and IDS: Using IPS and IDS together for Defense in Depth [en línea]. GSEC Practical v1.4b, Option 1, SANS Institute InfoSec Reading Room, February 23, 2004. Disponible en Internet: URL <https://www.sans.org/reading-room/whitepapers/detection/understanding-ips-ids-ips-ids-defense-in-depth-1381>.

ISACA, Marco de Riesgo de TI. [en línea]. Isaca. Disponible en Internet: URL<http://www.colmich.edu.mx/computo/files/MAAGTIC/risk_it_framework.pdf#page42>

KIBIRKSTIS, Algis. What is The Role of a SIEM in Detecting Events of Interest. [en línea]. SANS IDFAQ, November 2009. Disponible en internet: URL<https://www.sans.org/security-resources/idfaq/what-is-the-role-of-a-siem-in-detecting-events-of-interest/5/10>.

MELL, Peter; SCARFONE, Karen, National Institute of Standards and Technology y ROMANOSKY, Sasha. Carnegie Mellon University A Complete Guide to the Common Vulnerability Scoring System Version 2.0. [en línea]. CVSS, June 2007. Disponible en internet: URL< https://www.first.org/cvss/cvss-v2-guide.pdf>

MUY SEGURIDAD.NET. Roban 12 millones de dólares tras hackear un banco de Ecuador. [en línea]. Muy Seguridad.net. Mayo 24, 2016 Disponible en Internet: URL <http://muyseguridad.net/2016/05/24/roban-12-millones-dolares-hackear-banco-ecuador/>

NIST, National Institute of Standards and Technology. National Vulnerability Database. [en línea]. Common Vulnerability Scoring System Version 2 Calculator. Disponible en Internet: URL<https://nvd.nist.gov/cvss.cfm?calculator&adv&version=2>

PROTEKTNET, Pruebas de Penetración. [en línea]. Protektnet. Disponible en Internet: URL<https://protektnet.com/servicios/analisis-de-seguridad/pruebas-de-penetracion/>

SANS Institute InfoSec Reading Room, PKI, The What, The Why, and The How. [en línea]. SANS. Disponible en Internet: URL<https://www.sans.org/reading-room/whitepapers/vpns/pki-what-why-764>.

SANS, Securing the Human. Defining the Security Awareness Maturity Model. [en línea]. SANS. Mar 8, 2016 Disponible en Internet: URL<https://securingthehuman.sans.org/blog/2016/03/08/defining-the-security-awareness-maturity-model>

SECURITY, TechCenter. Security Bulletin Severity Rating System. [en línea]. Security, TechCenter. May, 2012. Disponible en Internet: URL< https://technet.microsoft.com/es-es/security/gg309177.aspx>

SUPERINTENDENCIA Financiera de Colombia. Requerimientos mínimos de seguridad y calidad para la realización de operaciones. Circular Externa 042 de 2012 [en línea]. Superintendencia Financiera de Colombia. Octubre, 2012. Disponible en Internet: URL< http://www.certicamara.com/download/correspondencia/20121005_Anexos_12_circular_042_de_2012.pdf>

ANEXO A

DETERMINACIÓN DEL IMPACTO

En los cuadros 12 al 53 se muestra la medición de Impacto para cada vulnerabilidad; se subrayó en colores la valoración de cada variable (afectación amenaza-criticidad del activo), así como el resultado del cálculo del impacto con el fin de identificar gráficamente cada valor, el color rojo indica un valor alto, el color amarillo indica un valor medio y el color verde indica un valor bajo:

Cuadro 12. Impacto servidor Server vulnerabilidad “Infección de servidor”

Impacto			Afectación por la amenaza		
			Infección de servidor		
			Bajo	Medio	Alto
Criticidad del activo	**Server**	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 13. Impacto servidor Server vulnerabilidad “Volcado de contenido de memoria RAM”

Impacto			Afectación por la amenaza		
			Volcado de contenido de memoria RAM		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 14. Impacto servidor Server vulnerabilidad “Volcado de memoria RAM a través de programas ejecutados a través de RDP-compartir recursos locales”

Impacto			Afectación por la amenaza		
			Volcado de memoria RAM a través de programas ejecutados a través de RDP-compartir recursos locales.		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 15. Impacto servidor Server vulnerabilidad “Versión de oracle database obsoleta”

Impacto			Afectación por la amenaza		
			Versión de oracle database obsoleta		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 16. Impacto 550 PC'S vulnerabilidad “Acceso BIOS sin contraseña”

Impacto			Afectación por la amenaza		
			Acceso BIOS sin contraseña		
			Bajo	Medio	Alto
Criticidad del activo	PCs	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 17. Impacto 550 PC'S vulnerabilidad "Arranque de equipo de escritorio con otro sistema operativo"

Impacto			Afectación por la amenaza		
			Arranque de equipo de escritorio con otro sistema operativo		
			Bajo	Medio	Alto
Criticidad del activo	PCs	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 18. Impacto servidor Server "Versión de Microsoft Windows Server 2003 obsoleta"

Impacto			Afectación por la amenaza		
			Versión de Microsoft Windows Server 2003 obsoleta		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 19. Impacto servidor Server "Sesiones CIFS NULL permitidas"

Impacto			Afectación por la amenaza		
			Sesiones CIFS NULL permitidas		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 20. Impacto servidor Server “Sesiones CIFS NULL permitidas”

Impacto			Afectación por la amenaza		
			Sesiones CIFS NULL permitidas		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 21. Impacto servidor Server “Sesiones CIFS NULL permitidas”

Impacto			Afectación por la amenaza		
			Sesiones CIFS NULL permitidas		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 22. Impacto servidor Server “Sesiones CIFS NULL permitidas”

Impacto			Afectación por la amenaza		
			Sesiones CIFS NULL permitidas		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 23 Impacto servidor Server “Sesiones CIFS NULL permitidas”

Impacto			Afectación por la amenaza		
			Sesiones CIFS NULL permitidas		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 24. Impacto servidor Server “Sesiones CIFS NULL permitidas”

Impacto			Afectación por la amenaza		
			Sesiones CIFS NULL permitidas		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 25. Impacto servidor Server “Acceso no autorizado explotando vulnerabilidades del servicio VNC remote control.”

Impacto			Afectación por la amenaza		
			Acceso no autorizado explotando vulnerabilidades del servicio VNC remote control.		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 26. Impacto servidor Server “Denegación de servicio por vulnerabilidad: apache HTTPD: range header remote DoS.”

Impacto			Afectación por la amenaza		
			Denegación de servicio por vulnerabilidad: apache HTTPD: range header remote DoS		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 27. Impacto servidor Server “Denegación de servicio por vulnerabilidad: apache HTTPD: range header remote DoS.”

Impacto			Afectación por la amenaza		
			Denegación de servicio por vulnerabilidad: apache HTTPD: range header remote DoS		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 28. Impacto servidor Server “Suplantación de cuentas de usuario a través de SMB”

Impacto			Afectación por la Amenaza		
			Suplantación de cuentas de usuario a través de SMB.		
			Bajo	Medio	Alto
Criticidad del Activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 29. Impacto servidor server “Suplantación de cuentas de usuario a través de SMB”

Impacto			Afectación por la Amenaza		
			Suplantación de cuentas de usuario a través de SMB.		
			Bajo	Medio	Alto
Criticidad del Activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 30. Impacto servidor Server “Suplantación de cuentas de usuario a través de SMB”

Impacto			Afectación por la amenaza		
			Suplantación de cuentas de usuario a través de SMB.		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 31. Impacto servidor Server “Suplantación de cuentas de usuario a través de SMB”

Impacto			Afectación por la amenaza		
			Suplantación de cuentas de usuario a través de SMB.		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 32. Impacto servidor Server “Interceptación de tráfico por vulnerabilidad OpenSSL SSL/TLS MITM”

Impacto			Afectación por la amenaza		
			Interceptación de tráfico por vulnerabilidad OpenSSL SSL/TLS MITM		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 33. Impacto servidor Server “Servidor TLS/SSL soporta SSLv2 y SSLv3”

Impacto			Afectación por la amenaza		
			Servidor TLS/SSL soporta SSLv2 y SSLv3		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 34. Impacto servidor Server “Interceptación de tráfico por suplantación de certificado”

Impacto			Afectación por la amenaza		
			Interceptación de tráfico por suplantación de certificado		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 35. Impacto servidor Server “Interceptación de tráfico por algoritmos cipher débiles servidor TLS/SSL”

Impacto			Afectación por la amenaza		
			Interceptación de tráfico por algoritmos cipher débiles servidor TLS/SSL		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 36. Impacto servidor Server “Interceptación de tráfico por cifrado RC4 en protocolo SSL”

Impacto			Afectación por la amenaza		
			Interceptación de tráfico por Cifrado RC4 en protocolo SSL		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 37. Impacto servidor SERVER “Interceptación de tráfico por suplantación de certificado”

Impacto			Afectación por la amenaza		
			Interceptación de tráfico por suplantación de certificado		
			Bajo	Medio	Alto
Criticidad del activo	SERVER	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 38. Impacto Cuentas del dominio de la organización vulnerabilidad “Acceso no autorizado por contraseñas débiles”

Impacto			Afectación por la amenaza		
			Acceso no autorizado por contraseñas débiles		
			Bajo	Medio	Alto
Criticidad del Activo	Cuentas del dominio de la organización	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 39. Impacto 550 PC'S “Volcado de contenido de memoria RAM (local y remoto) y obtención de credenciales almacenadas en procesos a partir del volcado.”

Impacto			Afectación por la amenaza		
			1) Volcado de contenido de memoria RAM (local y remoto) 2) Obtención de credenciales almacenadas en procesos		
			Bajo	Medio	Alto
Criticidad del activo	PCs	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 40. Impacto Server “Volcado de contenido de memoria RAM (local y remoto) y obtención de credenciales almacenadas en procesos a partir del volcado.”

Impacto			Afectación por la amenaza		
			1) Volcado de contenido de memoria RAM (local y remoto) 2) Obtención de credenciales almacenadas en procesos		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto

Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León

Cuadro 41. Impacto Server “Volcado de contenido de memoria RAM (local y remoto) y obtención de credenciales almacenadas en procesos a partir del volcado.”

Impacto			Afectación por la amenaza		
			1) Volcado de contenido de memoria RAM (local y remoto) 2) Obtención de credenciales almacenadas en procesos		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 42. Impacto PC “Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”

Impacto			Afectación por la amenaza		
			Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”		
			Bajo	Medio	Alto
Criticidad del activo	PC	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 43. Impacto PC “Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”

Impacto			Afectación por la amenaza		
			Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”		
			Bajo	Medio	Alto
Criticidad	PC	Bajo	Bajo	Bajo	Medio

del activo		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 44. Impacto 550 PC'S “Escalada de privilegios mediante cuentas administradoras locales "XXXXX" "XXXXX" "XXX" "XXXXX" "XXXX”

Impacto			Afectación por la amenaza		
			Escalada de privilegios mediante cuentas administradoras locales "XXXXX" "XXXXX" "XXX" "XXXXX" "XXXX"		
			Bajo	Medio	Alto
Criticidad el activo	PCs	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 45. Impacto 550 PC'S “Escalada de privilegios mediante cuenta administradora de dominio usuario: "XXXX", "XXXXX", "inv”

Impacto			Afectación por la amenaza		
			Escalada de privilegios mediante cuenta Administradora de dominio usuario: "XXXX", "XXXXX", "inv"		
			Bajo	Medio	Alto
Criticidad del activo	PCs	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 46. Impacto servidor Server “Múltiples vulnerabilidades en IBM WebSphere Application Server 6.1”

Impacto			Afectación por la amenaza		
			Múltiples vulnerabilidades en IBM WebSphere Application Server 6.1		
			Bajo	Medio	Alto
Criticidad	Server	Bajo	Bajo	Bajo	Medio

del activo		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 47. Impacto servidor Server “Interceptación de tráfico a través de Microsoft Windows RDP Man in The Middle”

Impacto			Afectación por la amenaza		
			Interceptación de tráfico a través de Microsoft Windows RDP Man in The Middle		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 48. Impacto servidor Server “Interceptación de tráfico a través de Microsoft Windows RDP Man in The Middle”

Impacto			Afectación por la amenaza		
			Interceptación de tráfico a través de Microsoft Windows RDP Man in The Middle		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 49. Impacto 500PC’s “Acceso no autorizado al sistema por usuario administrador local sin contraseña”

Impacto			Afectación por la amenaza		
			Acceso no autorizado al sistema por usuario administrador local sin contraseña		
			Bajo	Medio	Alto
Criticidad	Desktop's	Bajo	Bajo	Bajo	Medio

del activo		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 50. Impacto servidor Server “Credenciales por defecto o fáciles de averiguar "Quest Software"

Impacto			Afectación por la amenaza		
			Credenciales por defecto o fáciles de averiguar "Quest Software"		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 51. Impacto servidor Server “Control sobre el sistema operativo desde la base de datos"

Impacto			Afectación por la amenaza		
			Control sobre el sistema operativo desde la base de datos		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 52. Impacto servidor Server “Transmisión de información sin cifrar”

Impacto			Afectación por la amenaza		
			Transmisión de información sin cifrar		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto

		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

Cuadro 53. Impacto servidor Server “Múltiples vulnerabilidades en oracle database server”

Impacto			Afectación por la amenaza		
			Múltiples vulnerabilidades en oracle database server		
			Bajo	Medio	Alto
Criticidad del activo	Server	Bajo	Bajo	Bajo	Medio
		Medio	Bajo	Medio	Alto
		Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León					

ANEXO B

DETERMINACIÓN DEL RIESGO

En los cuadros 54 al 96 se muestra el cálculo del riesgo para cada vulnerabilidad; se subrayó en colores la valoración de cada variable (Impacto – Probabilidad de ocurrencia), así como el resultado del cálculo del riesgo con el fin de identificar gráficamente cada valor, el color rojo indica un valor alto, el color amarillo indica un valor medio y el color verde indica un valor bajo:

Cuadro 54. Riesgo alto servidor Server vulnerabilidad “Infección de servidor”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 55. Riesgo alto servidor Server vulnerabilidad “Vulnerabilidad volcado de contenido de memoria RAM-obtención Tickets de Kerberos válidos”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 56. Riesgo alto servidor Server vulnerabilidad “Volcado de memoria RAM a través de programas ejecutados a través de RDP-compartir recursos locales.”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 57. Riesgo alto servidor Server vulnerabilidad “Versión de oracle database obsoleta”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 58. Riesgo medio 550 PC'S vulnerabilidad “Acceso BIOS sin contraseña”

Riesgo 550 PC'S		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 59. Riesgo medio 550 PC'S vulnerabilidad “Arranque de equipo de escritorio con otro sistema operativo”

Riesgo 550 PC'S		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 60. Riesgo alto servidor Server “Versión de Microsoft Windows Server 2003 obsoleta”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 61. Riesgo medio servidor Server “Sesiones CIFS NULL permitidas”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 62. Riesgo medio servidor Server “Sesiones CIFS NULL permitidas”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 63. Riesgo alto servidor Server “Sesiones CIFS NULL permitidas”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 64. Riesgo alto servidor Server “Sesiones CIFS NULL permitidas”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 65. Riesgo alto servidor Server “Sesiones CIFS NULL permitidas”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 66. Riesgo alto servidor Server “Sesiones CIFS NULL permitidas”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 67. Riesgo alto servidor Server “Acceso no autorizado explotando vulnerabilidades del servicio VNC remote control.”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 68. Riesgo alto servidor Server “Denegación de servicio por vulnerabilidad: apache HTTPD: range header remote DoS.”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 69. Riesgo medio servidor Server “Denegación de servicio por vulnerabilidad: apache HTTPD: range header remote DoS.”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 70. Riesgo bajo servidor Server “Suplantación de cuentas de usuario a través de SMB.

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 71. Riesgo medio servidor Server “Suplantación de cuentas de usuario a través de SMB.

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 72. Riesgo bajo servidor Server “Suplantación de cuentas de usuario a través de SMB.

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 73. Riesgo bajo servidor Server “Suplantación de cuentas de usuario a través de SMB”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 74. Riesgo bajo servidor Server “Interceptación de tráfico por vulnerabilidad OpenSSL SSL/TLS MITM”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 75. Riesgo medio servidor Server “Servidor TLS/SSL soporta SSLv2 y SSLv3”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 76. Riesgo alto servidor Server “Interceptación de tráfico por suplantación de certificado”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 77. Riesgo medio servidor Server “Interceptación de tráfico por algoritmos cipher débiles servidor TLS/SSL”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 78. Riesgo medio servidor Server “Interceptación de tráfico por cifrado RC4 en protocolo SSL”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 79. Riesgo alto servidor SERVER “Interceptación de tráfico por suplantación de Certificado”

Riesgo Srv SERVER		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 80. Riesgo alto Cuentas del dominio de la organización “Acceso no autorizado por contraseñas débiles”

Cuentas del dominio de la organización		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 81. Riesgo bajo 550 PC'S “Volcado de contenido de memoria RAM (local y remoto) y obtención de credenciales almacenadas en procesos a partir del volcado.”

Riesgo 550 PC'S		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 82. Riesgo alto Server “Volcado de contenido de memoria RAM (local y remoto) y Obtención de credenciales almacenadas en procesos a partir del volcado.”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 83. Riesgo alto Server “Volcado de contenido de memoria RAM (local y remoto) y obtención de credenciales almacenadas en procesos a partir del volcado.”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 84. Riesgo alto Server “Volcado de contenido de memoria RAM (local y remoto) y obtención de credenciales almacenadas en procesos a partir del volcado.”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 85. Riesgo medio PC “Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”

Riesgo PC		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 86. Riesgo medio PC “Escalada de privilegios en sistema operativo de equipo de escritorio mediante “Teclas especiales”

Riesgo PC		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 87. Riesgo medio 550 PC'S “Escalada de privilegios mediante cuentas administradoras locales "XXXXX" "XXXXX" "XXX" "XXXXX” “XXXX”

Riesgo 550 PC'S		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 88. Riesgo medio 550 PC'S “Escalada de privilegios mediante cuenta administradora de dominio usuario: "XXXX", "XXXXX", "inv”

Riesgo 550 PC'S		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 89. Riesgo alto servidor Server “Múltiples vulnerabilidades en IBM WebSphere Application Server 6.1”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 90. Riesgo bajo servidor Server “Interceptación de tráfico a través de Microsoft Windows RDP Man in The Middle”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 91. Riesgo bajo servidor Server “Interceptación de tráfico a través de Microsoft Windows RDP Man in The Middle”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 92. Riesgo medio 500PC’s “Acceso no autorizado al sistema por usuario administrador local sin contraseña”

Riesgo 500PC’s		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 93. Riesgo bajo servidor Server “Credenciales por defecto o fáciles de averiguar "Quest Software"

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 94. Riesgo medio servidor Server “Control sobre el sistema operativo desde la base de datos"

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 95. Riesgo bajo servidor Server “Transmisión de información sin cifrar”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

Cuadro 96. Riesgo alto servidor Server “Múltiples vulnerabilidades en oracle database server”

Riesgo Srv Server		Impacto		
		Bajo	Medio	Alto
Probabilidad de ocurrencia	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León				

ANEXO C

EVALUACIÓN Y VIABILIDAD TÉCNICA DE LOS CONTROLES RECOMENDADOS A IMPLEMENTAR PARA SOLUCIONAR Y/ O MITIGAR CADA VULNERABILIDAD

A.1 SERVIDOR SERVER VULNERABILIDAD INFECCIÓN DE SERVIDOR

A.1.1 Identificación del control. La vulnerabilidad Identificada por el fabricante fue la siguiente:

"A través de acceso remoto no autorizado y sin la detección del antivirus, instalar un malware (ejecutable con extensión EXE) diseñado específicamente para la prueba de intrusión. Esto se realizó sobre el servidor de dominio x.x.x.x y permitió habilitar un servicio de SSH sobre este."[23]

El control propuesto por el fabricante es el siguiente:

Se debe impedir la copia y ejecución de programas que no se encuentren en la lista de los permitidos por el sistema en todos los servidores y equipos de escritorio como por ejemplo, la protección "System LockDown" del producto Symantec End point Protection.

A.1.2 Viabilidad del control propuesto. De acuerdo a la validación realizada en conjunto con Gerencia de Telemática No es posible implementar la característica "System Lock Down" de Symantec ya que este configuración consiste en bloquear todos los archivos del sistema operativo a excepción de una lista blanca alimentada de manera manual, lo anterior se debe a que en el ambiente del banco existen variables de entorno que cambian en razón al tiempo, principalmente la instalación de parches de seguridad de Windows y políticas de dominio como wallpapers, fondos de pantallas entre otros, implementar este control impide la distribución de este tipo de políticas de seguridad del Banco.

[23] XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016

Se determinó implementar a través del Symantec una política para bloquear aplicaciones y algunos archivos ejecutables no usados en el Banco.

Así mismo para evitar los posibles vectores de infección se configurara el bloqueo de correos entrantes con adjuntos que contengan extensiones de ejecutables; también se bloqueara la descarga de ejecutables a través de la navegación WEB.

A.2 SERVIDOR SERVER (CONTROLADOR DE DOMINIO) VULNERABILIDAD VOLCADO DE CONTENIDO DE MEMORIA RAM-OBTENCIÓN TICKETS DE KERBEROS VÁLIDOS

A. 2.1 Identificación del control. La vulnerabilidad Identificada por el fabricante fue la siguiente:

"Se diseñó un script para que una vez se ejecute, abra el terminal cmd.exe con permisos de administrador y ejecute el programa para volcado de memoria para así guardar la información en un archivo y ruta especifica en el disco duro.

Se lograron capturar 541 Tickets de Kerberos validos del dominio, de usuarios administradores, servidores y otros. Es posible utilizar estos Tickets inyectándolos durante una sesión, y así poder acceder a los recursos y derechos de los usuarios a los que pertenecen (es posible inyectar varios Tickets Kerberos al mismo tiempo, y así obtener una “súper sesión” [24]

El control propuesto por el fabricante es el siguiente:

Revisar la configuración de Tickets en Kerberos para que estos tengan un tiempo de renovación limitada a algunas horas.

A.2.2 Viabilidad del control propuesto. De acuerdo a la validación realizada en conjunto con Gerencia de Infraestructura y Microsoft se definieron los siguientes parámetros a implementar para la vigencia de los tickets de Kerberos:

[24] XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016

- Maximum Lifetime for Service Ticket: 10 horas
- Maximum Lifetime: 7 días
- Maximum Tolerance for Computer Clock Synchronization: 5 min.
- Maximum lifetime for user ticket renewal 7 days

Adicional a esto se implementara en el Antivirus Symantec una política para bloquear aplicaciones y algunos archivos ejecutables no usados en el Banco

A.3 SERVIDOR SERVER VULNERABILIDAD VOLCADO DE MEMORIA RAM A TRAVÉS DE PROGRAMAS EJECUTADOS A TRAVÉS DE RDP - COMPARTIR RECURSOS LOCALES

A.3.1 Identificación del control. La vulnerabilidad Identificada por el fabricante fue la siguiente:

"Utilizando la opción de compartir recursos locales de un equipo durante una sesión RDP se copió y ejecuto en el servidor de dominio terciario una herramienta que permitió realizar un volcado de memoria, obteniendo la siguiente información: Se lograron capturar varias credenciales de cuentas de administradores del dominio"[25]

EL control propuesto por el fabricante es el siguiente:

Realizar una modificación en las políticas del dominio para que se restringa el uso de "compartir recursos locales" durante conexiones RDP con servidores.

A.3.2 Viabilidad del control propuesto. De acuerdo a la validación realizada en conjunto con Gerencia de Infraestructura y Microsoft se definió la aplicación de una GPO que modifique los parámetros de configuración de la aplicación de terminal server "mstsc" de Microsoft para que no permita habilitar los recursos compartidos en las conexiones RDP.

[25] XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016

A.4 SERVIDOR SERVER VULNERABILIDAD VERSIÓN DE ORACLE DATABASE OBSOLETA

A.4.1 Identificación del control. La vulnerabilidad Identificada por el fabricante fue la siguiente:

"El servidor con la dirección IP x.x.x.x tiene instalada y en uso una versión de Oracle Database Server obsoleta, la cual es vulnerable a diferentes tipos de ataques.

Las versiones obsoletas de Oracle pueden ser vulnerables a ataques de Buffer overflow, Inyecciones SQL, Cross Site Scripting, y Directory Traversal.

Se detectó lo siguiente en el servidor:

- Servicio Oracle TNS Listener detectado
- Versión vulnerable del software Oracle Database detectada: Oracle Database 10.2.0.4." [26]

El control propuesto por el fabricante es el siguiente:

Actualizar a la versión disponible el software Oracle Database.

A.4.2 Viabilidad del control propuesto. De acuerdo a la validación realizada en conjunto con Gerencia de Infraestructura y la Gerencia de Desarrollo se viene realizando la migración del motor de Base de datos a la versión Oracle 11g Enterprise desde Enero del 2017.

A.5 SERVIDOR SERVER VULNERABILIDAD VERSIÓN DE MICROSOFT WINDOWS SERVER 2003 OBSOLETA

[26] XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016

A.5.1 Identificación del control. La vulnerabilidad Identificada por el fabricante fue la siguiente:

"Se detectó la versión Microsoft Windows Server 2003 SP2 en servidores de la organización. El soporte de Microsoft para todas las versiones de Windows Server 2003 finalizo el 14 de Julio de 2015.Las versiones de Windows sin soporte pueden contener vulnerabilidades sin parchar.

Un atacante podría descubrir y explotar vulnerabilidades presentes en el sistema operativo, y de esta forma impactar en la confidencialidad, disponibilidad e integridad de su información."[27]

El control propuesto por el fabricante es el siguiente:

Actualizar el Sistema Operativo por uno que tenga soporte activo, como Windows Server 2012.

A.5.2 Viabilidad del control propuesto. De acuerdo a la validación realizada en conjunto con Gerencia de Infraestructura este servidor tiene fecha de migración para Noviembre de 2017 según el proyecto de migración de servidores Windows 2003; sin embargo se ajustó la fecha debido al riesgo identificado

A.6 SERVIDOR SERVER- SERVER- SERVER- SERVER VULNERABILIDAD SESIONES CIFS NULL PERMITIDAS

A.6.1 Identificación del control. La vulnerabilidad Identificada por el fabricante fue la siguiente:

"Las sesiones NULL permiten a usuarios anónimos establecer sesiones CIFS sin autenticación con implementaciones Windows, Samba, o Solaris; fue posible extraer:

- Las políticas de contraseñas y de cuentas de usuarios del dominio.

[27] XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016

- Las cuentas de usuarios activas en los hosts.
- Los grupos activos en los hosts.
- RPC endpoints.

Hay que tener en cuenta que deshabilitar las sesiones NULL puede tener un impacto negativo en la funcionabilidad, ya que algunas aplicaciones y entornos de red podrían depender de estas últimas para su operación. Ver el siguiente artículo de Microsoft para más información: Microsoft Knowledge Base Article 823659"[28]

El control propuesto por el fabricante es el siguiente:

Cambiar el valor de la siguiente llave de registro a “1” para bloquear la enumeración de SAM y de las cuentas de usuarios, y prohíbe a una sesión NULL de poder ver las cuentas de usuarios y recursos compartidos. Si se ingresa el valor “2” se deshabilita el acceso de las sesiones NULL sin permisos explícitos.

Key Name: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA
Value Name: RestrictAnonymous
Type: DWORD
Value: 0

A.6.2 Viabilidad del control propuesto. De acuerdo a la validación realizada en conjunto con Gerencia de Infraestructura se definió implementar la llave de registro:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA
Value Name: RestrictAnonymous
Type: DWORD
Value: 0

A.7 SERVIDOR SERVER VULNERABILIDAD ACCESO NO AUTORIZADO EXPLOTANDO VULNERABILIDADES DEL SERVICIO VNC REMOTE CONTROL

[28] XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016

A.7.1 Identificación del control. La vulnerabilidad identificada por la empresa de seguridad externa es la siguiente:

"Un servidor VNC provee acceso remoto a usuarios que lo requieran en el host donde está instalado. Si el servicio llega a ser comprometido, un atacante podría obtener control total del sistema, el software VNC fue evidenciado instalado en el servidor x.x.x.x-Server"[29].

Al respecto, el control recomendado por la empresa de seguridad externa es:

Utilizar un servicio más seguro y robusto. Es importante recordar que un servidor VNC utiliza contraseñas troncadas a 8 bytes durante la autenticación, volviéndolo vulnerable a ataques de fuerza bruta. Con la tecnología existente seria relativamente fácil para un atacante.

A.7.2 Viabilidad del control propuesto. Se realiza validación en conjunto entre el área de Seguridad Informática y la Gerencia de Infraestructura respecto al software VNC instalado sobre el servidor, luego de explicar los riesgos de poder materializarse un ataque mediante el uso de este software para conexión remota se acordó acatar la recomendación del proveedor y por común acuerdo se eliminara el software instalado.

De igual forma se acordó que si se requiere tener acceso remoto al servidor, la conexión se realice haciendo uso del servicio de RDP propio de Windows, con los permisos de conexión previamente definidos y limitados.

A.8 SERVIDOR SERVER VULNERABILIDAD DENEGACIÓN DE SERVICIO POR VULNERABILIDAD: APACHE HTTPD RANGE HEADER REMOTE DOS

[29] XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016

A.8.1 Identificación del control. La vulnerabilidad identificada por la empresa de seguridad externa es la siguiente:

"El filtro byterange en el Servidor Apache HTTP v1.3.x, v2.0.x hasta v2.0.64, y v2.2.x hasta v2.2.19 permite a atacantes remotos provocar una denegación de servicio (consumo de memoria y CPU) a través de una cabecera Range que expresa múltiple rangos de solapamiento. Se encontró que el servidor Server responde con un contenido parcial a una petición enviada con una cabecera Range maliciosa"[30].

Al respecto, el control recomendado por la empresa de seguridad externa es:

"Actualizar Apache HTTPD a la última versión disponible".

A.8.2 Viabilidad del control propuesto. Se realizó validación conjunta con el área de Desarrollo del Banco a quien se les expuso la amenaza encontrada y el riesgo expuesto que se tiene con la versión del Apache instalada en este servidor. El área de desarrollo nos informa que actualmente están llevando a cabo la migración de contenedores a WebLogic por ser un servidor de aplicaciones mucho más eficientes, de igual forma conforme al plan de migración el servidor Server se migró en Enero de 2017 a otro servidor con WebLogic, por lo que el servidor de Server se dará de baja posterior a la migración.

Por lo anterior la recomendación dada por el proveedor aunque es válida no será tomada en cuanta por el Banco, ya que esta vulnerabilidad al realizar la migración de contenedor queda subsanada.

A.9 SERVER VULNERABILIDAD INTERCEPTACIÓN DE TRÁFICO POR SUPLANTACIÓN DE CERTIFICADO

[30] XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016

A.9.1 Identificación del control. La vulnerabilidad identificada por la empresa de seguridad externa es la siguiente:

"El certificado X.509 del servidor no está firmado por una autoridad de certificación pública conocida. Este fallo podría facilitar el llevar a cabo el robo de información transmitida entre un cliente legítimo y el servidor remoto. Al revisar el certificado SSL del servidor x.x.x.x- Server se observa que no pertenecen a una entidad certificadora conocida:

x.x.x.x:8071:
TLS/SSL certificate signed by unknown, untrusted CA: CN=x.x.x.x, O="Server, Inc.", OU=Server Engineering, L=San Diego, ST=California, C=US -- Path does not chain with any of the trust anchors"[31]

Al respecto, el control recomendado por la empresa de seguridad externa es:

Adquirir o generar un certificado apropiado para este servicio.

A.9.2 Viabilidad del control propuesto. El servidor en el que fue detectado por el puerto 8071 no posee un certificado generado por la CA interna del Banco, corresponde a una de las interfaces de la plataforma de filtro de contenido WEB del Banco del fabricante Tripware. Esta herramienta actualmente es administrada por el área de Seguridad Informática donde se fue gestionada la remediación o posibles remediaciones de la misma.

Luego de realizar las respectivas validaciones junto con el fabricante se encontró que esta herramienta carece de características que permitan cargar certificados digitales en interfaces específicas, además de no permitir la des habilitación de protocolos SSLv2 y SSLv3, tampoco es posible configurar la herramienta para que solo permita conexiones TLS superiores a 1.0, al igual que la versión de OpenSSL utilizada no es posible actualizarse.

Por lo anterior y en base a otros problemas operativos presentados por la herramienta, esta solución de filtrado de contenido WEB se migrara a otra solución del fabricante Mcafee Web Gateway, por lo cual una vez la plataforma sea migrada quedaría subsanada la vulnerabilidad reportada.

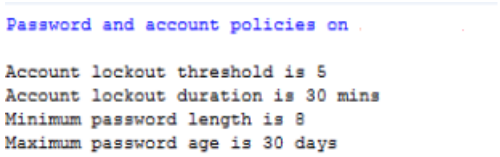
[31] XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016

A.10 CUENTAS DEL DOMINIO DE LA ORGANIZACIÓN VULNERABILIDAD ACCESO NO AUTORIZADO POR CONTRASEÑAS DÉBILES

A.10.1 Identificación del control. La vulnerabilidad identificada por la empresa de seguridad externa es la siguiente:

"Las contraseñas de acceso a servidores deben poseer características que permitan ser en sí mismas un elemento adicional de seguridad, una longitud adecuada (mayor a 12) y el uso de caracteres alfanuméricos que incluyan números, minúsculas, mayúsculas y caracteres especiales, ayudan a evitar el éxito frente a ataques de fuerza bruta o de diccionario. El acceso a los servidores puede permitir la fuga de información sensible como datos de clientes, bases de datos, etc. En la figura 4 se muestra la política de definición de contraseñas del dominio encontrada.

Figura 4. Política de definición de contraseñas de dominio encontrada



Fuente: Informe Prueba de Intrusión

De igual forma se identificaron varias contraseñas de cuentas de usuarios del dominio que tienen una longitud de 9 caracteres, los cuales incluían únicamente números y letras en minúsculas"[32].

Al respecto, el control recomendado por la empresa de seguridad externa es:

Hacer uso de contraseñas con las siguientes características:

- Letras mayúsculas
- Letras minúsculas

[32] XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016

- Caracteres Especiales
- Números
- Longitud mínima de 12 caracteres
- Evitar secuencias de números o letras
- Evitar palabras que puedan encontrarse en el diccionario
- No usar fechas, años ni nombres de personas o entidades

Para usuarios de dominio se debe aumentar la complejidad de políticas de contraseñas y adicionalmente crear una lista de contraseñas no permitidas, así como un historial.

A.10.2 Viabilidad del control propuesto. En conjunto con el área de Seguridad de la Información se ha definido realizar los ajustes necesarios en la Política de Contraseñas del Banco, de acuerdo a lo sugerido.

De igual forma para que este control pueda ser implementado y cumplido por los usuarios también se requirió llegar a un acuerdo junto con la Gerencia de Telemática de poder implementar los ajustes en la configuración del directorio de xxxx (herramienta del Banco para administración de cuentas de accesos), en la cual se exigirá a los usuarios cuando cambie las contraseñas que cumpla con los parámetros establecidos, también se incluirá un listado de palabras de diccionario para que sean excluidas como posibles passwords.

A.11 SERVIDOR SERVER VULNERABILIDAD VOLCADO DE CONTENIDO DE MEMORIA RAM (LOCAL Y REMOTO) Y OBTENCIÓN DE CREDENCIALES ALMACENADAS EN PROCESOS A PARTIR DEL VOLCADO

A.11.1 Identificación del control. La vulnerabilidad identificada por la empresa de seguridad externa es la siguiente:

“Fue posible obtener credenciales en texto claro de diferentes cuentas de usuarios locales o de dominio realizando volcados de memoria en los diferentes equipos accedidos durante las pruebas

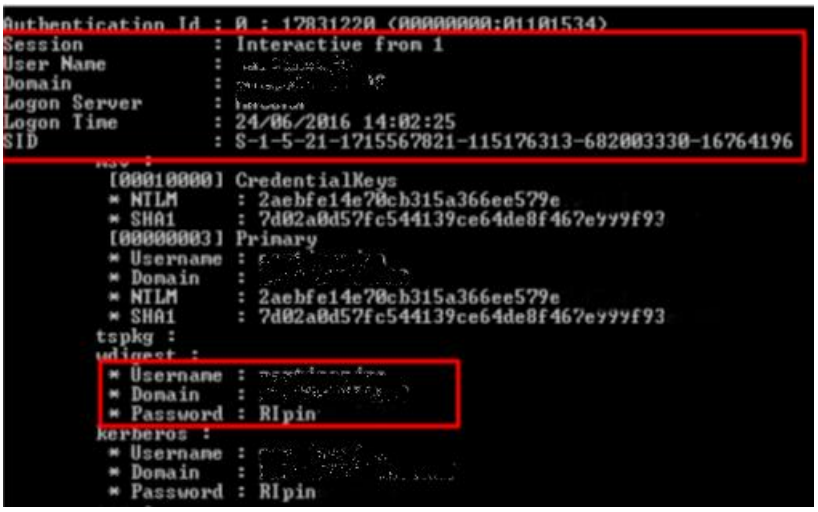
- Volcado de memoria local en equipo de escritorio

Se extrajeron credenciales en texto claro de usuarios del dominio que utilizaron el equipo de escritorio suministrado por el cliente.

Se aprovechó el acceso al disco duro del equipo de escritorio que se obtuvo al inicio de las pruebas para realizar una modificación en el S.O. que permite obtener un terminal de comandos con derechos de administrador presionando una combinación de teclas. También, se copió en él una herramienta que permite realizar un volcado de la memoria del equipo.
El siguiente paso fue esperar que un usuario del dominio se autentique en el equipo, bloquee su sesión (Tecla Windows + L) y se aleje para no ser observado.

Después, las credenciales del usuario residiendo en la memoria RAM, se utilizó el terminal de comandos cmd.exe con derechos administrativos obtenido previamente, para realizar el volcado de memoria:
Este ataque puede ser realizado en cualquier equipo de la empresa al que se tenga acceso físico, solo hay que esperar que el usuario autenticado en el equipo bloquee su sesión. Se obtuvieron las credenciales en texto claro del usuario de dominio llamado “xxxx” como se muestra en el Figura 5:

Figura 5. Obtención de credenciales en texto plano



Fuente: Informe Prueba de Intrusión

- Volcado de memoria remoto en equipos de escritorio

Se extrajeron credenciales en texto claro de usuarios del dominio los equipo de escritorio accedidos remotamente, utilizando el usuario administrador local llamado “XXXXX” y los otros usuarios obtenidos durante los ataques anteriores.

Aprovechando el acceso administrador remoto a los diferentes equipos de escritorio, se realizó un volcado de memoria en estos últimos y fue posible obtener en texto claro las credenciales de todos los usuarios que permanecían en memoria como se muestra en la Figura 6.

Figura 6. Extracto de credenciales obtenidas en texto claro

Fuente: Informe Prueba de Intrusión.

Por ejemplo, fue posible acceder al equipo de escritorio que posee la dirección ip x.x.x.x y cuyo nombre es XXXXX. Aprovechando el acceso remoto obtenido con el usuario XXXXX se realizó un volcado de su memoria RAM, y de esta forma se obtuvieron en texto claro las credenciales del usuario del dominio ENTIDAD llamado: “xxxx”.

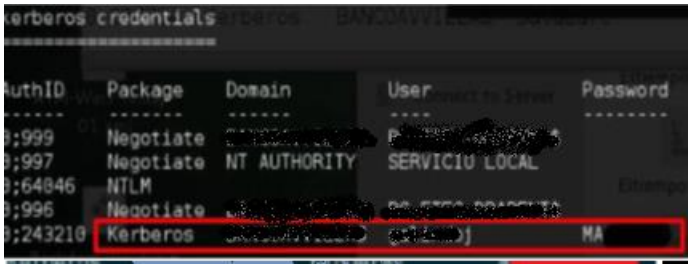
También se obtuvieron en texto claro las credenciales de la cuenta “XXXX” como se muestra en la Figura 7, la cual corresponde al usuario de loggeo de servicios de la solución “XXXX”.

Figura 7. Volcado de memoria

Fuente: Informe Prueba de Intrusión

De igual manera, se realizó un volcado de memoria en el equipo de escritorio que posee la dirección IP x.x.x.x, en la Figura 8 se observa las credenciales obtenidas de kerberos en texto claro del usuario de dominio llamado “xxxxx”, el cual estaba autenticado en el equipo en ese momento.

Figura 8. Volcado de memoria y obtención de credenciales en texto claro



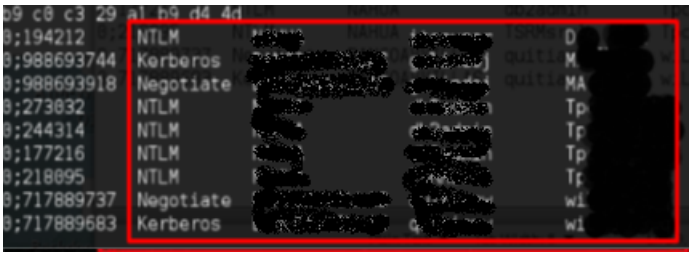
Fuente: Informe Prueba de Intrusión

- Volcado de memoria en Servidor de Base de Datos

Utilizando el equipo que posee la dirección ip x.x.x.x como pivote, y el usuario de dominio obtenido en este último durante el volcado de memoria realizado, fue posible obtener en texto claro todas las credenciales presentes en la memoria del servidor objetivo conteniendo la base de datos xx.

Aprovechando el acceso administrador obtenido mediante el usuario “xxx” se realizó un volcado de memoria en el servidor SERVER, la figura 9 muestra las credenciales obtenidas en texto claro de los usuarios locales llamados “xxx”, “xxx” y “xxx”, así como las credenciales en texto claro del usuario de domino “xxx””[33].

Figura 9. Volcado de memoria en el servidor x.x.x.x



Fuente: Informe Prueba de Intrusión

Al respecto, el control recomendado por la empresa de seguridad externa es:

Aplicar el parche del fabricante 2871997 en el servidor de dominio el cual posee el S.O. Windows Server 2008 R2, para mejorar la protección y la gestión de las credenciales. https://support.microsoft.com/en-us/kb/2871997.

Actualizar el S.O. del servidor de dominio a la versión Windows Server 2012 R2, para utilizar el grupo de usuarios llamado: Protected User Security Group.

[33] XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016

A.11.2 Viabilidad del control propuesto. Ya que actualmente el servidor Server es Windows Server 2008 se analiza la primera opción recomendada por el proveedor.

En la Tabla 37 se detalla el análisis realizado al KB 2871997:

Tabla 37. Características del KB 2871997

Item	Característica
Fecha de publicación	12/05/2014
Sistemas Operativos	Windows 7, Windows Server 2008 R2, Windows 8 y Windows Server 2012
Objetivo	Actualización para mejorar los controles para la protección y la administración de credenciales para reducir el robo de credenciales.
Resumen	Esta solución Fix it cambia la clave del Registro **UseLogonCredential** para que las contraseñas WDigest no se almacenen en la memoria. Después de instalar la actualización de seguridad 2871997 y de aplicar seguidamente esta solución Fix it a los sistemas que ejecutan Windows 7, Windows Server 2008 R2, Windows 8 o Windows Server 2012, ya no debería tener almacenadas en la memoria credenciales básicas (de texto sin cifrar).
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

De acuerdo a lo validado en conjunto con la Gerencia de Infraestructura quienes, administran los servidores del banco y de acuerdo a la importancia y recomendación de instalación del parche 2871997 se acordó viable su implementación. Ya que con esta instalación se mitigaría la obtención de credenciales que son almacenadas en la cache del equipo.

A.12 SERVIDOR SERVER VULNERABILIDAD VOLCADO DE CONTENIDO DE MEMORIA RAM (LOCAL Y REMOTO) Y OBTENCIÓN DE CREDENCIALES ALMACENADAS EN PROCESOS A PARTIR DEL VOLCADO

A.12.1 Identificación del control. La vulnerabilidad identificada por la empresa de seguridad externa es la siguiente:

“Fue posible obtener credenciales en texto claro de diferentes cuentas de usuarios locales o de dominio realizando volcados de memoria en los diferentes equipos accedidos durante las pruebas.

- Volcado de memoria local en equipo de escritorio

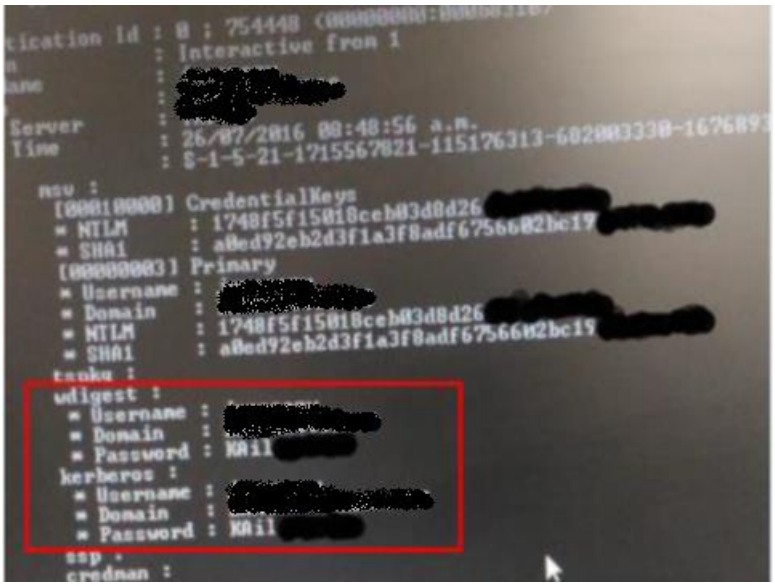
Se extrajeron credenciales en texto claro de usuarios del dominio que utilizaron el equipo de escritorio suministrado por el cliente.

Se aprovechó el acceso al disco duro del equipo de escritorio que se obtuvo al inicio de las pruebas para realizar una modificación en el S.O. que permite obtener un terminal de comandos con derechos de administrador presionando una combinación de teclas. También, se copió en él una herramienta que permite realizar un volcado de la memoria del equipo.

El siguiente paso fue esperar que un usuario del dominio se autentique en el equipo, bloquee su sesión (Tecla Windows + L) y se aleje para no ser observado.
Después, las credenciales del usuario residiendo en la memoria RAM, se utilizó el terminal de comandos cmd.exe con derechos administrativos obtenido previamente, para realizar el volcado de memoria:

Este ataque puede ser realizado en cualquier equipo de la empresa al que se tenga acceso físico, solo hay que esperar que el usuario autenticado en el equipo bloquee su sesión. En la figura 10 se evidencia las credenciales obtenidas en texto claro del usuario de dominio llamado “xxxx”:

Figura 10. Obtención de credenciales en texto plano



Fuente: Informe Prueba de Intrusión

- Volcado de memoria remoto en equipos de escritorio

Se extrajeron credenciales en texto claro de usuarios del dominio y usuarios locales de los equipo de escritorio accedidos remotamente, utilizando el usuario administrador local llamados “XXXXX” obtenido previamente.

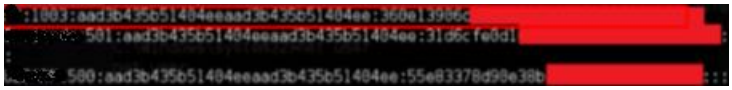
Aprovechando el acceso administrador remoto a los diferentes equipos de escritorio, se realizó un volcado de memoria en estos últimos, en la figura 11 se evidencia que fue posible obtener en texto claro las credenciales de todos los usuarios que permanecían en memoria.

Figura 11. Extracto de credenciales obtenidas en texto claro

Fuente: Informe Prueba de Intrusión

Por ejemplo, fue posible acceder al equipo de escritorio que posee la dirección IP x.x.x.x, y cuyo nombre es “xxxx”. Aprovechando el acceso remoto obtenido con el usuario “XXXXX”, se obtuvo el hash del usuario administrador local llamado “xxx”, como se puede observar en la figura 12:

Figura 12. Obtención de hash del usuario admin local “xxx” en equipo de escritorio x.x.x.x



Fuente: Informe Prueba de Intrusión

También, se realizó un volcado de su memoria RAM, y de esta forma se obtuvieron en texto claro las credenciales de los usuarios del dominio llamados “xxx” y “xxxx”, como se muestra en la figura 13.

Figura 13. Volcado de memoria y obtención de credenciales de texto claro

Fuente: Informe Prueba de Intrusión

A continuación, se utilizó el usuario administrador local llamado “xx” previamente obtenido para autenticarse en el equipo de escritorio que posee la dirección IP x.x.x.x, el cual pertenece a un usuario xx. Se realizó un volcado de memoria y en la figura 14 se muestra las credenciales kerberos obtenidas en texto claro del usuario de dominio llamado “xxxx”, el cual estaba autenticado en el equipo en ese momento:

Figura 14. Volcado de memoria y obtención de credenciales de texto claro

Fuente: Informe Prueba de Intrusión

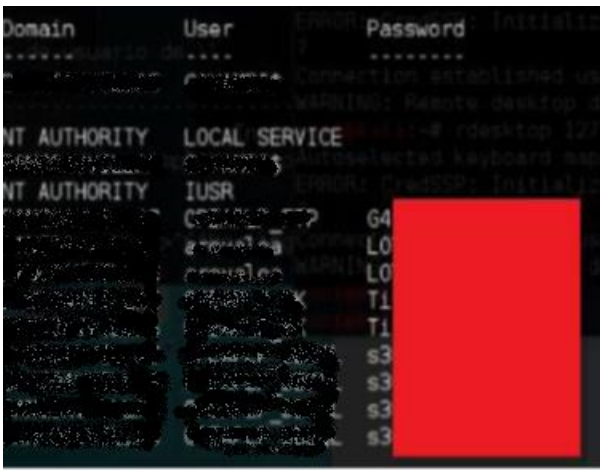
Este usuario se utilizara para acceder al servidor de bases de datos objetivo de las pruebas llamado “Server”.

- Volcado de memoria en servidor de base de datos

Utilizando el equipo que posee la dirección IP x.x.x.x como pivote, y el usuario de dominio obtenido en este último durante el volcado de memoria realizado, fue posible obtener en texto claro todas las credenciales presentes en la memoria del servidor objetivo conteniendo la base de datos xxx.

Aprovechando el acceso administrador obtenido mediante el usuario “xxxx”, se realizó un volcado de memoria en el servidor Server (IP x.x.x.x), en la figura 15 se evidencia las credenciales obtenidas en texto claro de los usuarios del dominio llamados “xxxx”, “xxxx” “xxxx”, y “xxxxx”[34].

Figura 15. Volcado de memoria en el servidor x.x.x.x



Fuente: Informe Prueba de Intrusión

Al respecto, el control recomendado por la empresa de seguridad externa es:

[34] XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016.

“Aplicar el parche del fabricante 2871997 en el servidor de dominio el cual posee el S.O. Windows Server 2008 R2, para mejorar la protección y la gestión de las credenciales. https://support.microsoft.com/en-us/kb/2871997.

Actualizar el S.O. del servidor de dominio a la versión Windows Server 2012 R2, para utilizar el grupo de usuarios llamado: Protected User Security Group.”

A.12.2 Viabilidad del control propuesto. Ya que actualmente el servidor Server es Windows Server 2008 se analiza la primera opción recomendada por el proveedor.

En la Tabla 38 se detalla el análisis realizado al KB 2871997:

Tabla 38. Características del KB 2871997

Item	**Característica**
Fecha de publicación	12/05/2014
Sistemas Operativos	Windows 7, Windows Server 2008 R2, Windows 8 y Windows Server 2012
Objetivo	Actualización para mejorar los controles para la protección y la administración de credenciales para reducir el robo de credenciales.
Resumen	Esta solución Fix it cambia la clave del Registro **UseLogonCredential** para que las contraseñas WDigest no se almacenen en la memoria. Después de instalar la actualización de seguridad 2871997 y de aplicar seguidamente esta solución Fix it a los sistemas que ejecutan Windows 7, Windows Server 2008 R2, Windows 8 o Windows Server 2012, ya no debería tener almacenadas en la memoria credenciales básicas (de texto sin cifrar).
Fuente: Autores Ana María Sossa López, Harvey Enrique Melo León	

De acuerdo a lo validado en conjunto con la Gerencia de Infraestructura quienes, administran los servidores del banco y de acuerdo a la importancia y recomendación de instalación del parche 2871997 se acordó viable su implementación. Ya que con esta instalación se mitigaría la obtención de credenciales que son almacenadas en la cache del equipo.

A.13 SERVIDOR SERVER VULNERABILIDAD MÚLTIPLES VULNERABILIDADES EN IBM WEBSPHERE APPLICATION SERVER 6.1

A.13.1 Identificación del control. La vulnerabilidad identificada por la empresa de seguridad externa es la siguiente:

“A raíz de la detección de la versión exacta del software IBM WebSphere Application Server 6.1, ésta posee diferentes vulnerabilidades que ponen en peligro la seguridad de los sistemas. Debido a la existencia de múltiples vulnerabilidades en el software afectado, un atacante podría:

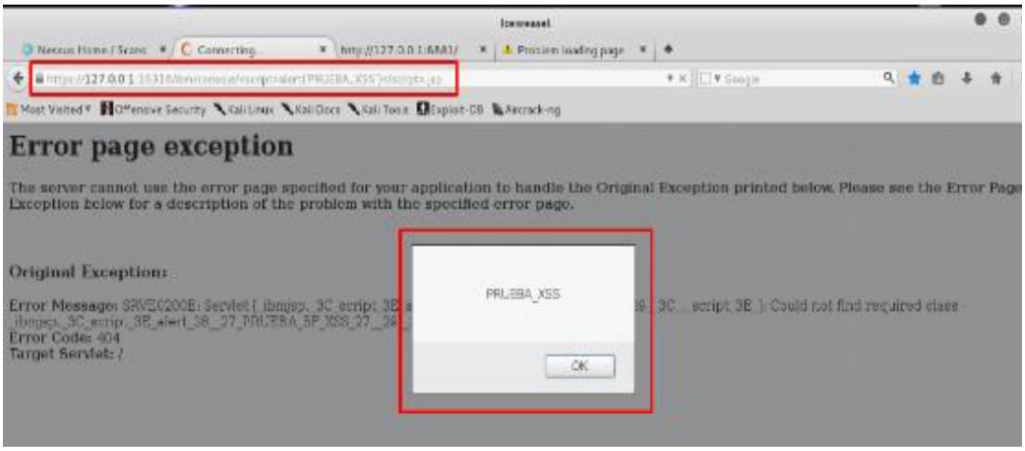
- Provocar una denegación de servicio
- Acceso a información sensible
- Realizar ataques de XSS.
- Escalar privilegios del sistema

Para demostrar la presencia de esta versión del software vulnerable, se realizó la explotación de un Cross Site Scripting presente en la página de la consola de IBM WebSphere Application Server.

Para logarlo, se utilizó el equipo de escritorio que posee la dirección IP x.x.x.x como pivote, ya que tiene visibilidad al servidor objetivo de las pruebas (x.x.x.x). Después se abrió un navegador, en este caso Iceweasel, y se abrió en este último la URL de la consola incluyendo el payload malicioso:
https://x.x.x.x:16316/ibm/console/<script>alert(‘PRUEBA_XSS’)</script>.jsp

En la figura 16 aparece la dirección de localhost 127.0.0.1 ya que se realizó una redirección de puertos del servidor objetivo hacia el equipo de escritorio utilizado por el consultor, mediante el equipo utilizado como pivote:

Figura 16. Explotación de XSS en servidor



Fuente: Informe Prueba de Intrusión

Se puede observar la explotación del XSS en ventana del navegador.
También, en la figura 17 se puede evidenciar la versión del software vulnerable en el “banner” mostrado por el servidor[35]:

Figura 17. Versión del software 6.1.0.5 del servidor.

```
Installed version : 6.1.0.5
Fixed version : 6.1.0.33
```

Fuente: Informe Prueba de Intrusión Red

Al respecto, el control recomendado por la empresa de seguridad externa es:

[35] XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016

- Se recomienda mantener el software actualizado, ya sea mediante parches de seguridad o instalando las versiones más recientes del producto.
- Si se utiliza el software WebSphere Application Server, aplicar el Fix Pack 33 (6.1.0.33) o posterior.
- Si se utiliza el paquete embebido de WebSphere Application Server con Tivoli Directory Server, aplicar el ultimo Fix Pack eWAS recomendado."

A.13.2 Viabilidad del control propuesto. Se realiza validación en conjunto con el área de Desarrollo quienes confirman que el servidor Server tiene un WebSphere Application Server y debido a las múltiples vulnerabilidades asociadas a la versión instalada, indican que es viable y factible aplicar el parche correspondiente para mitigar los riesgos asociados a dicha versión. De igual forma nos indican que el parche debe ser instalado en ambiente de pruebas de forma inicial y debe estar desplegado por 2 meses con el fin de verificar que no afecte producción y una vez cumplido este tiempo en ventana programada se realizar la instalación del parche 33 (6.1.0.33) en ambiente productivo.

A.14 SERVIDOR SERVER VULNERABILIDAD MÚLTIPLES VULNERABILIDADES EN ORACLE DATABASE SERVER

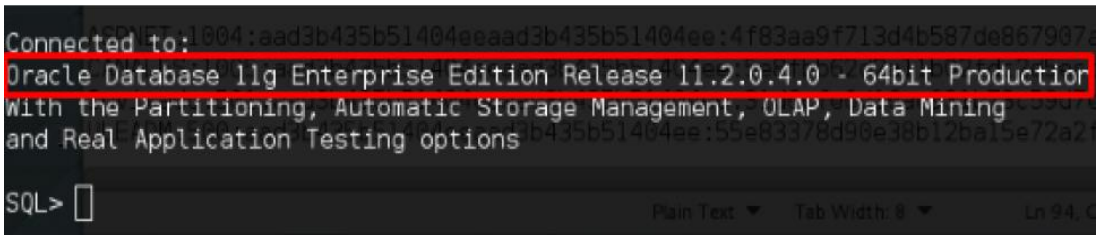
A.14.1 Identificación del control. La vulnerabilidad identificada por la empresa de seguridad externa es la siguiente:

"A raíz de la detección de la versión exacta del software Oracle Database Server, ésta posee diferentes vulnerabilidades que ponen en peligro la seguridad de los sistemas. Debido a la existencia de múltiples vulnerabilidades en el software afectado, un atacante podría:

- Provocar una denegación de servicio
- Ejecutar código en el servidor de forma remota
- Escalar privilegios en el sistema

Toda la información aquí expuesta está basada únicamente en el "banner" mostrado por el servidor, como se puede observar en la Figura 18"[36].

Figura 18. Respuesta del servidor indicando la versión del software 11.2.0.4.0



Fuente: Informe Prueba de Intrusión

Al respecto, el control recomendado por la empresa de seguridad externa es:

Se recomienda mantener el software actualizado, ya sea mediante parches de seguridad o instalando las versiones más recientes del producto.

A.14.2 Viabilidad del control propuesto. Se socializa la vulnerabilidad reportada con la Gerencia de Infraestructura y la dirección de los Administradores de Bases de Datos ya que la vulnerabilidad hace referencia a la versión de Base de Datos instalada sobre el servidor de Server que una Oracle Database 11g.

Conforme a las validaciones de los riesgos que un atacante podría producir sobre bases de datos de producción, se acepta la recomendación del proveedor y se consideran viable la instalación del Critical Pach Update: cpuapr2016v3-2985753 la cual subsana múltiples vulnerabilidades que afectan la versión de Oracle 11g.

[36] XXXXX, Colombia. Informe de pruebas de intrusión. [Confidencial]. Octubre 2016.

Elaboración de un plan de remediación a las vulnerabilidades críticas identificadas a partir de una prueba de intrusión a la infraestructura tecnológica de una entidad bancaria

Sossa López. Ana María - Melo León. Harvey Enrique
Especialización en Seguridad Informática - Universidad Piloto de Colombia

***Abstract*—El objetivo del presente trabajo muestra cómo elaborar un plan de remediación a las vulnerabilidades críticas identificadas en una prueba de intrusión.**

Para la elaboración del plan de remediación se desarrolló una metodología que permite identificar el riesgo asociado a cada vulnerabilidad reportada, permitiendo priorizar la remediación de las vulnerabilidades que representan un alto riesgo para el Banco, así como definir los controles que deben ser implementados para mitigar los riesgos garantizando que el riesgo residual cumpla con los niveles aceptables de riesgo determinados por la entidad.

***Index Terms*—Pruebas de Intrusión, Gestión de Riesgo, Vulnerabilidades, Amenaza, Riesgo, Riesgo residual, Impacto, CVSS.**

I. INTRODUCCIÓN

Las entidades prestadoras de bienes y servicios financieros en busca de brindar un mejor servicio a los consumidores y con miras a incrementar su participación en el mercado, constantemente acondicionan sus procesos, servicios, canales electrónicos e infraestructura tecnológica, con el fin de apoyar las necesidades del negocio.

Desde lo propio de la Infraestructura de TI, las entidades constantemente acondicionan su infraestructura tecnológica de tal forma que sea posible apoyar las iniciativas estratégicas de la entidad, esto conlleva a cambios en el estado de seguridad de los componentes de TI, así como deterioro en los controles de seguridad implementados, por lo cual y en cumplimiento de la legislación Colombiana (Circular 042 Superintendencia Financiera de Colombia)[1] las entidades anualmente realizan como mínimo una prueba de intrusión a los componentes de infraestructura tecnológica con el fin de identificar los nuevos riesgos de Seguridad de la Información que puedan ser materializados.

A diferencia de un análisis de vulnerabilidades, una prueba de Intrusión tiene como objetivo comprobar la materialización del riesgo por medio de la explotación de las vulnerabilidades y/o debilidades identificadas por una entidad externa experta en seguridad, sobre los componentes de infraestructura tecnológica; esto permite conocer el estado y efectividad real de los controles de seguridad existentes, así como identificar las oportunidades de mejora que deben ser implementadas en los controles de seguridad establecidos, con el fin de evitar que la infraestructura tecnológica sea comprometida por un atacante mal intencionado afectando la confidencialidad, integridad y disponibilidad de la información.

II. QUÉ ES UNA PRUEBA DE INTRUSIÓN

Las pruebas de intrusión se realizan con el objetivo de medir el nivel de seguridad y madurez de los controles implementados en una organización a fin de evitar accesos no autorizados a los sistemas operativos, aplicaciones o bases de datos y a su información confidencial. Las pruebas de intrusión tienen la capacidad de simular el alcance que puede llegar a tener un potencial atacante de forma remota o local sobre la infraestructura de una entidad, el cual busca explotar de forma activa las vulnerabilidades de seguridad de dicha infraestructura

Las pruebas de intrusión se realizan en un ambiente controlado que permita simular un ataque permitiendo conocer el nivel de seguridad de la entidad, así:

- Nivel de Tolerancia: Resistencia de los sistemas a ataques que no afecten su funcionamiento.
- Nivel de Complejidad: Grado de dificultad de los ataques para afectar un sistema.

[1] SUPERINTENDENCIA Financiera de Colombia. Requerimientos mínimos de seguridad y calidad para la realización de operaciones. Circular Externa 042 de 2012 [en línea]. Superintendencia Financiera de Colombia. Octubre, 2012. Disponible en Internet: URL< http://www.certicamara.com/download/correspondencia/20121005_Anexos_12_circular_042_de_2012.pdf>

- Nivel de Detección: Capacidad de la infraestructura de seguridad para detectar los ataques[2].

Los alcances de las pruebas de penetración están dados por el éxito obtenido al evadir los controles de red implementados, escalar privilegios, realizar análisis e identificación de servicios y a su vez identificar las vulnerabilidades asociadas en los sistemas y redes de la infraestructura tecnológica.

Para el desarrollo de las pruebas de intrusión en la entidad se siguen las siguientes fases y ciclos los cuales van desde realizar un descubrimiento de la infraestructura, conocer sus activos críticos hasta llegar a realizar la explotación de las vulnerabilidades descubiertas[3].

FASE I: Evasión de controles de acceso a la red
FASE II: Escalar privilegios de forma remota
FASE III: Descubrimiento de activos y servicios
FASE IV: Inspección y explotación de vulnerabilidades

III. SISTEMA DE CALIFICACIÓN DE VULNERABILIDADES DE ACUERDO AL CVSS 2.0

El Common Vulnerability Scoring System (CVSS) proporciona un marco de referencia para comunicar características e impacto de las vulnerabilidades del área de TI. CVSS está bajo la custodia del Foro de respuesta a Incidentes y equipo de Seguridad (FIRST), sin embargo es un estándar abierto y libre.

Sin embargo, todos los anteriores sistemas aunque tienen un enfoque único para todas las vulnerabilidades asumen que el impacto de la materialización de una vulnerabilidad es constante y similar para cada organización.

El valor agregado al utilizar como guía el CVSS para determinar la criticidad de una vulnerabilidad son las métricas opcionales que provee el CVSS, métricas que evalúan los cambios en el tiempo que puedan tener las vulnerabilidades y los atributos propios del entorno del cliente donde aplica la vulnerabilidad.

Existen tres grupos de métricas usados por el CVSS para realizar la evaluación de las vulnerabilidades y cada uno maneja su propio conjunto de métricas, cuyo propósito es definir y comunicar las características fundamentales de una vulnerabilidad[4]:

- Métrica Base: Representa las características fundamentales de una vulnerabilidad que es constante en el tiempo y en el entorno de usuario.
- Métrica Temporal: Representa los cambios en el tiempo de las característica de una vulnerabilidad pero no en el entorno de usuario.
- Métrica de Entorno: Representa las características relevantes y únicas de una vulnerabilidad para un entorno de usuario en particular y específico.

La puntuación de cada Métrica es un valor entre 0 y 10 con los cuales se calcula un valor Overall que corresponde a la Métrica que posea mayor peso de las Métricas evaluadas. A continuación en la Figura 1 se muestran las métricas que se evalúan en cada grupo:

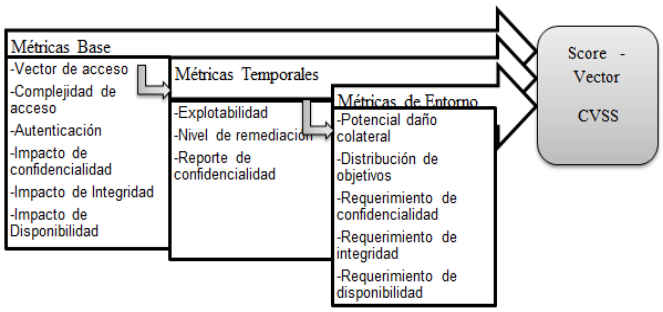


Fig. 1. Métricas CVSS V2.0

Para la métrica Base el score lo ayudan a determinar la información encontrada en los boletines de análisis de vulnerabilidades, vendedores de aplicaciones o productos de seguridad, sin embargo para las otras métricas Temporal y de Entorno el valor de score lo determina solamente el usuario respecto a su propio entorno.

Para determinar la severidad de las vulnerabilidades se utilizó la clasificación cuantitativa-cualitativa de severidad empleada por la NVD (National Vulnerability Database)5, la cual tiene tres niveles cualitativos relacionados con una escala cuantitativa de 0 a 10 como se muestra en la siguiente tabla.

TABLA I

CALIFICACIONES DE LA SEVERIDAD DE LAS VULNERABILIDADES

SEVERIDAD – NVD	CALIFICACIÓN - CVSS
Baja	0.0 – 3.9
Media	4.0 – 6.9
Alta	7.0 – 10.0

IV. METODOLOGÍA DE GESTIÓN DE RIESGO

[2] PROTEKTNET, Pruebas de Penetración. [en línea]. Protektnet. Disponible en Internet: URL<https://protektnet.com/servicios/analisis-de-seguridad/pruebas-de-penetracion/>

[3] Informe de pruebas de intrusión Memorando Interno de la entidad 0302-MEM-00102-15-121[Confidencial]

[4] MELL, Peter; SCARFONE, Karen, National Institute of Standards and Technology y ROMANOSKY, Sasha. Carnegie Mellon University A Complete Guide to the Common Vulnerability Scoring System Version 2.0. [en línea]. CVSS, June 2007. Disponible en internet: URL< https://www.first.org/cvss/cvss-v2-guide.pdf>

5 National Vulnerability Database. [en línea]. Common Vulnerability Scoring System Version 2 Calculator. Disponible en Internet: URL<https://nvd.nist.gov/cvss.cfm?calculator&adv&version=2>

La metodología ISO 27005 establece un proceso iterado de gestión de riesgos de seguridad de la información que contiene las siguientes actividades:

- Establecimiento del contexto.
- Valoración del riesgo.
- Tratamiento del riesgo.
- Aceptación del riesgo.
- Comunicación del riesgo.
- Monitoreo y revisión continua de los riesgos

A. Establecimiento del contexto

Esta actividad consiste en definir el alcance y los límites de la gestión de riesgos de Seguridad de la Información, basándose en los objetivos, procesos y funciones de negocio, así como la estructura de la organización, requisitos legales, normativos y políticas de la organización.

La norma recomienda desarrollar el contexto a partir de los siguientes enfoques:

- Evaluación de riesgos.
- Criterios de Impacto.
- Criterios de Aceptación de Riesgos.

Algunos ejemplos de contexto puede ser una aplicación del negocio, infraestructura tecnológica, un proceso de negocio, etc

B. Valoración del riesgo

La valoración del riesgo consta de tres actividades:

- Identificación del riesgo. Busca determinar que evento podría suceder que cause perdida potencial, cómo, dónde y por qué podría ocurrir la pérdida, esto se realiza a partir de la identificación de activos, amenazas, controles existentes, vulnerabilidades y sus consecuencias.

- Estimación del riesgo: Puede ser cuantitativa o cualitativa o una combinación de ambas. En la estimación cualitativa se utiliza una escala de atributos calificativos para describir la magnitud de las consecuencias potenciales, por ejemplo: bajo, alta, media; y en la estimación cuantitativa se utiliza una escala de valores numéricos para calificar la magnitud de las consecuencias potenciales.

  La estimación del riesgo se realiza en base a la evaluación de consecuencias, la probabilidad de ocurrencia de los incidentes y su nivel de estimación (asignación de un valor).

- Evaluación de riesgo: Propiedades de la seguridad de la información y/o procesos de negocio. Si un criterio o proceso tiene importancia baja para la organización (por ejemplo la pérdida de confidencialidad), entonces todos los riesgos que tienen impacto sobre este criterio o proceso deben tener una consideración más baja a diferencia de otros.

C. Tratamiento del riesgo

Esta actividad consiste en seleccionar los controles para reducir, retener, evitar o transferir los riesgos, así como definir un plan para el tratamiento de riesgo. Las opciones para el tratamiento del riesgo se deben ser seleccionadas con base en la evaluación del riesgo, el costo esperado para implementar estas opciones y los beneficios esperados como resultado de tales opciones, las cuatro formas de tratar el riesgo no necesariamente funcionan de manera independiente, un riesgo pude ser tratado de múltiples formas de manera simultánea.

D. Aceptación del riesgo

Esta actividad comprende la toma de decisión de aceptar los riesgos y las responsabilidades de la decisión, los directivos de la entidad deben revisar y aprobar los planes propuestos para el tratamiento del riesgo y los riesgos residuales resultantes.

E. Comunicación del riesgo

Esta actividad trata acerca de informar, intercambiar y compartir con todas las partes involucradas los riesgos de la organización.

F. Monitoreo y revisión continúa de los riesgos

El proceso de gestión del riesgo se deberá monitorear, revisar y mejorar continuamente, según sea necesario y adecuado; se debe verificar con regularidad que los criterios utilizados para medir el riesgo aún son válidos y consistentes con los objetivos, las estrategias y las políticas del negocio, y que los cambios en el contexto del negocio se toman en consideración de manera adecuada durante el proceso de gestión del riesgo.

V. DISEÑO DEL PLAN DE REMEDIACIÓN

Para la elaboración del plan de remediación de las vulnerabilidades críticas se desarrolló la metodología mostrada en el siguiente esquema:

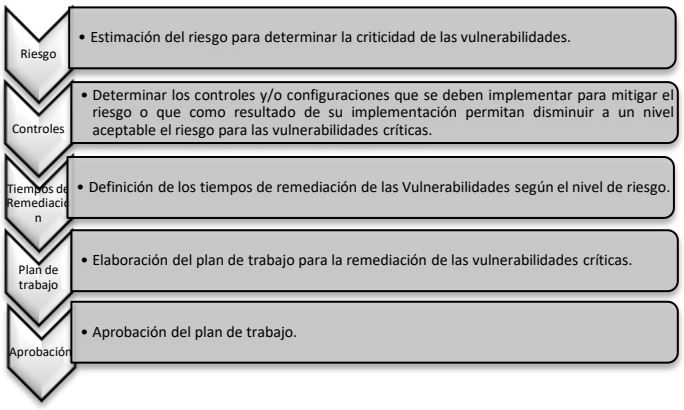


Fig. 2. Plan de Remediación

A continuación se indica cómo se logró cada uno de los procesos definidos anteriormente.

VI. VARIABLES DE INGENIERÍA PARA EL CÁLCULO DEL RIESGO

Para el cálculo del riesgo se siguen las siguientes mediciones que nos ayudan a encontrar la evaluación del riesgo asociado a cada vulnerabilidad reportada.

A. Cálculo del Riesgo

Es posible calcular el riesgo conociendo el impacto que tiene la materialización de una amenaza versus la probabilidad de que se materialice la misma, a continuación en la tabla II y III se muestra la clasificación y medición del riesgo respectivamente:

TABLA II

CLASIFICACION DEL RIESGO

RIESGO	
Alto	Riesgo alto
Medio	Riesgo medio
Bajo	Riesgo bajo

TABLA III

MEDICION DEL RIESGO

RIESGO		IMPACTO		
		Bajo	**Medio**	**Alto**
PROBABILIDAD OCURRENCIA	**Bajo**	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto

B. Cálculo del Impacto

El impacto corresponde a la medida del daño ocasionado sobre un activo de información como consecuencia de la materialización de una amenaza. Conociendo la importancia del activo y la afectación que causan las amenazas, es posible determinar el impacto, en la tabla IV y V se muestra la clasificación y medición del impacto respectivamente:

TABLA IV

CLASIFICACION DEL IMPACTO

IMPACTO	
Alto	Impacto alto
Medio	Impacto medio
Bajo	Impacto bajo

TABLA V

MEDICION DEL IMPACTO

IMPACTO		AFECTACIÓN DE LA VULNERABILIDAD EN EL ACTIVO DE INFORMACIÓN		
		Bajo	**Medio**	**Alto**
IMPORTANCIA DEL ACTIVO DE INFORMACIÓN	**Bajo**	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto

C. Importancia del activo

La importancia de los activos de información debe ser considerada y evaluada por cada organización dentro de un esquema de valoración del nivel de afectación del activo en cuanto a la disponibilidad, integridad y confidencialidad de la información que administra.

La clasificación de la importancia de los activos esta usualmente dada en términos cualitativos como alta, media y baja.

D. Afectación de la vulnerabilidad en el activo

Para determinar la afectación de las vulnerabilidades reportadas por la prueba de intrusión se utilizó como punto de partida la calificación dada en el reporte, la cual viene dada por el estándar del CVSS 2.0.

Sin embargo aunque el reporte solo indica la calificación de la métrica Base dada por CVSS, para efectos de resultados prácticos se calcularon las métrica Temporal y de Entorno con el fin de obtener un resultado promediado, el cual permitió reevaluar el nivel de afectación dado por el CVSS y ajustado al entorno evaluado.

E. Probabilidad de ocurrencia del evento

La probabilidad de ocurrencia se mide en relación a que tan frecuente es la materialización de una amenaza determinada, en la tabla VI se presenta el modelo de medición de la probabilidad

TABLA VI

PROBABILIDAD DE OCURRENCIA

VALOR	FRECUENCIA	CRITERIO
Alto	Muy frecuente	Cuando ha ocurrido más de 4 veces en año
Medio	Frecuente	Entre 2 y 4 veces en el año.
Bajo	Poco frecuente	Una vez cada 5 años

Con los anteriores resultados se obtiene la valoración del riesgo para cada una de las vulnerabilidades reportadas y conforme con el objetivo planteado la ejecución del plan de remediación se enfocara en las vulnerabilidades cuyo resultado fue una criticidad alta.

Esta metodología se aplicó para cada una de las vulnerabilidades reportadas en la prueba de intrusión obteniendo como resultado que al recalcular su criticidad se reduce en un 39% la cantidad de vulnerabilidades con criticidad alta.

VII. DETERMINACIÓN DE CONTROLES A IMPLEMENTAR

Con el fin de reducir el nivel de criticidad de las vulnerabilidades categorizadas con criticidad alta es importante evaluar y definir los controles y medidas a implementar teniendo en cuenta que estos controles puedan ser aplicados en el entorno tecnológico y los riesgos asociados a las vulnerabilidades estén dentro del criterio de aceptación del banco.

Por ello para analizar los controles se han establecido los siguientes pasos:

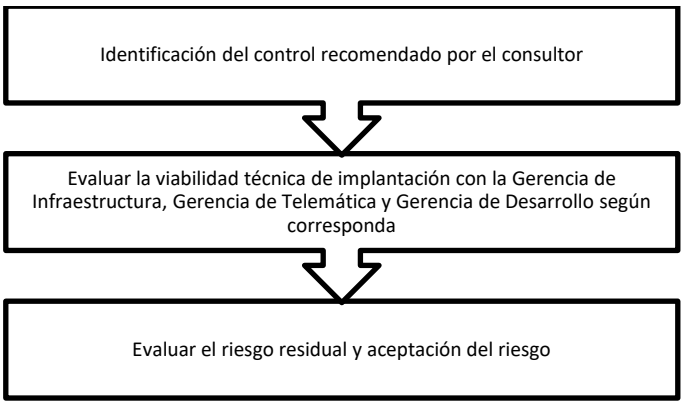


Fig. 3 Actividades definición controles a implementar

A. Identificación del control

En el informe entregado, la empresa externa proporciona el control propuesto por el fabricante para cada vulnerabilidad, este control muchas veces es difícil de aplicar en su totalidad ya que intervienen factores propios de la infraestructura tecnológica como: afectación de la operación, plataformas y/o software que no soportan los cambios, entre otras.

B. Evaluación de la viabilidad técnica

Por lo anterior, el área de Seguridad Informática del Banco lidera e investiga controles que remedien o mitiguen las acciones que puedan poner en riesgo la explotación de las vulnerabilidades. Los controles son evaluados y pactados con cada una de las áreas administradoras de los activos afectados, a fin de buscar la viabilidad y definir compromisos para la implementación de los controles.

C. Evaluar el riesgo residual

Riesgo residual. Se definió riesgo residual como la diferencia que existe entre el riesgo calculado y la efectividad de los controles implementados para reducir el riesgo; la fórmula matemática es detallada en la ecuación 1:

$$RiesgoResidual = RiesgoCalculado - \overline{X}EfectividadControles$$

Ecuación 1. Formula determinación del riesgo residual

Sin embargo y debido a que se busca que el riesgo residual sea una variable cuantitativa se establecen las siguientes relaciones y variables:

- La relación entre valor cualitativo y cuantitativo del riesgo calculado, a continuación en la tabla VII se presenta esta relación.

TABLA VI I

RELACIÓN ENTRE VALOR CUALITATIVO Y CUANTITATIVO DEL RIESGO

RIESGO CALCULADO	VALOR CUANTITATIVO
Alto	3
Medio	2
Bajo	1

- La relación entre el valor cualitativo y cuantitativo de la efectividad de los controles establecidos para mitigar los riesgos, a continuación en la tabla VIII muestra esta relación:

TABLA VIII

RELACIÓN ENTRE EL VALOR CUALITATIVO Y CUANTITATIVO DE LA EFECTIVIDAD DE LOS CONTROLES

EFECTIVIDAD DEL CONTROL	VALOR CUALITATIVO
Bajo	1
Medio	2
Alto	3

Cabe subrayar que a cada control acordado se le dio una calificación respecto a su efectividad, para luego promediarlos.

D. Aceptación del riesgo residual

Los criterios de aceptación de riesgo fueron definidos de acuerdo con los criterios presentados en la tabla IX:

TABLA IX

CRITERIOS DE ACEPTACION DEL RIESGO

NIVEL DE RIESGO RESIDUAL	CRITERIO DE ACEPTACIÓN	DESCRIPCIÓN
0 >= y =< 1	Aceptable	Reducción del riesgo Eliminación del riesgo Evasión del riesgo Transferencia del riesgo
1 >= y =< 2	No Aceptable	N/A
2 >= y =< 3	No Aceptable	N/A

Por lo que el banco solo aceptara el riesgo residual cuando su valor este entre 0 y 1. Si el resultado del riesgo residual está fuera de la escala definida como aceptable, el proceso de determinación de controles debe ser nuevamente evaluado.

VIII. DEFINICIÓN DE LOS TIEMPOS DE REMEDIACIÓN, ELABORACIÓN Y APROBACIÓN DEL PLAN DE TRABAJO

Es importante realizar un trabajo en conjunto con las áreas administradoras de los activos vulnerables con el fin de generar compromisos para aplicar los controles previamente definidos, como resultado, se obtiene el listado de las vulnerabilidades reportadas asociada a cada área involucrada las cuales pueden ser: Gerencia de Telemática, Gerencia de Infraestructura (Administradores de Bases de Datos y Servidores) o Gerencia de Desarrollo y frente a cada una la fecha de compromiso para aplicar el control propuesto y acordado.

Esto permite generar un control y asegurar que los planes de remediación sean aplicados en su totalidad, garantizando que las vulnerabilidades con nivel de criticidad alto sean reducidas y que esto no genere afectación a la normal operación de la infraestructura del Banco.

IX. CONCLUSIONES

Se construyó una metodología que permite tratar de manera eficiente las vulnerabilidades explotadas en la prueba de intrusión, priorizando el tratamiento de las amenazas que mayor impacto y probabilidad de ocurrencia pueden tener en el ambiente tecnológico del Banco.

La metodología propuesta para la gestión de vulnerabilidades críticas a partir del cálculo del riesgo, permite al Banco definir los controles que se deben implementar con el fin de garantizar la reducción del riesgo a niveles aceptables por el Banco, así como la aplicabilidad tecnológica del mismo.

Las vulnerabilidades reportadas por el proveedor son categorizadas respecto a su severidad según el estándar CVSS v2.0, sin embargo en esta calificación no se tuvo en cuenta la criticidad de los activos del Banco, la cantidad de equipos afectados, ambiente de producción o pruebas, entre otros, por lo cual se recalculo la severidad empleando las métricas base, temporal y de entorno definidas por el mismo estándar con el fin de establecer la severidad real aplicada al ambiente tecnológico del Banco, esta actividad permitió concluir que la métrica de entorno posee mayor porcentaje de ponderación respecto a las otras métricas, razón por la cual la severidad obtenida después del proceso aplicado difiere de la severidad reportada inicialmente por el proveedor.

Empleando la metodología propuesta se obtiene una diferencia del 39.2% entre las vulnerabilidades reportadas como críticas por el proveedor y las vulnerabilidades consideradas críticas para el Banco, esto tiene una importancia significativa para la Vicepresidencia de Operaciones y Tecnología del Banco, ya que algunos controles consisten en adquirir e implementar nuevas herramientas de seguridad como el filtro de contenido Web, así como la migración de algunas aplicaciones críticas para el Banco, lo cual sin este estudio no se hubiera asignado la celeridad adecuada.

Involucrar de manera directa a los responsables de la implementación del control desde la fase de evaluación y definición del mismo, permitió generar un plan de remediación que se ajusta a la realidad del Banco y su ambiente tecnológico, generando compromiso de las partes involucradas a fin de garantizar que no se generaran mayores incumplimientos en las fechas establecidas en dicho plan.

Gran parte de la metodología desarrollada en esta investigación fue diseñada con base en la norma ISO 27005, esta norma enmarca la gestión de riesgos de seguridad de la información para una organización ajustándose a los procesos definidos en la norma ISO 27001, sin embargo se puede concluir que es aplicable a micro procesos que requieren una valoración del riesgo como los procesos de gestión de vulnerabilidades, gestión de pruebas de penetración y/o procesos de gestión de incidentes.

REFERENCIAS

[1] SUPERINTENDENCIA Financiera de Colombia. Requerimientos mínimos de seguridad y calidad para la realización de operaciones. Circular Externa 042 de 2012 [en línea]. Superintendencia Financiera de Colombia. Octubre, 2012. Disponible en Internet: URL< http://www.certicamara.com/download/correspondencia/20121005_Anexos_12_circular_042_de_2012.pdf>

[2] PROTEKTNET, Pruebas de Penetración. [en línea]. Protektnet. Disponible en Internet: URLhttps://protektnet.com/servicios/analisis-de-seguridad/pruebas-de-penetracion/

[3] Informe de pruebas de intrusión

[4] MELL, Peter; SCARFONE, Karen, National Institute of Standards and Technology y ROMANOSKY, Sasha. Carnegie Mellon University A Complete Guide to the Common Vulnerability Scoring System Version 2.0. [en línea]. CVSS, June 2007. Disponible en internet: URL< https://www.first.org/cvss/cvss-v2-guide.pdf>

[5] National Vulnerability Database. [en línea]. Common Vulnerability Scoring System Version 2 Calculator. Disponible en Internet: URL<https://nvd.nist.gov/cvss.cfm?calculator&adv&version=2>